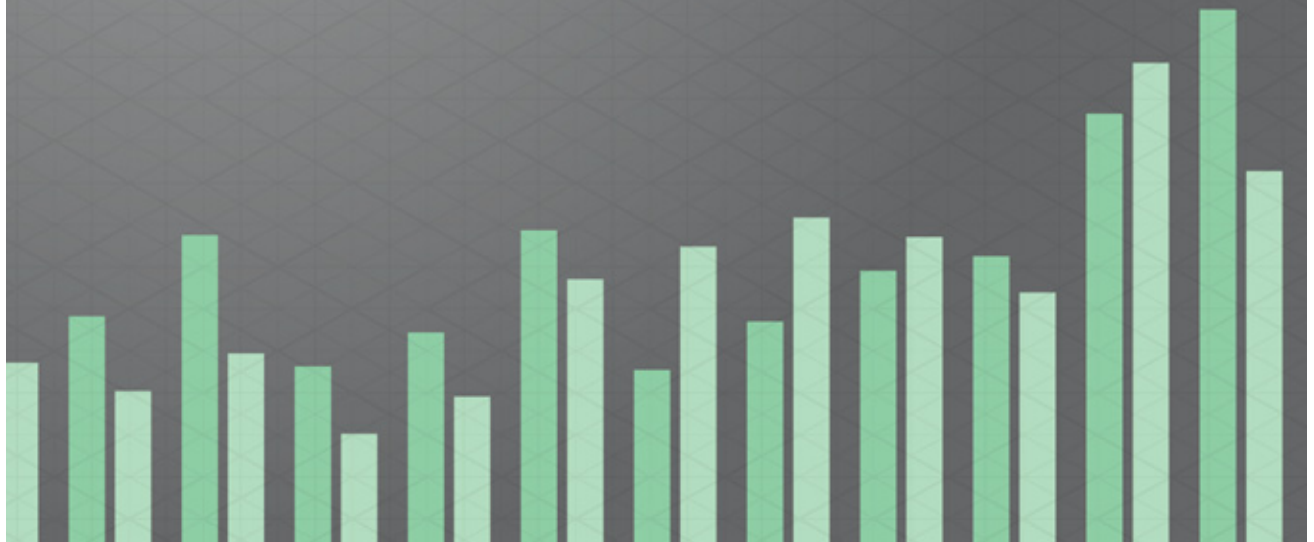




ACTUATE.
The BIRT Company™



BIRT Analytics



Administering BIRT Analytics

Information in this document is subject to change without notice. Examples provided are fictitious. No part of this document may be reproduced or transmitted in any form, or by any means, electronic or mechanical, for any purpose, in whole or in part, without the express written permission of Actuate Corporation.

© 2003 - 2015 by Actuate Corporation. All rights reserved. Printed in the United States of America.

Contains information proprietary to:
Actuate Corporation, 951 Mariners Island Boulevard, San Mateo, CA 94404

www.actuate.com

The software described in this manual is provided by Actuate Corporation under an Actuate License agreement. The software may be used only in accordance with the terms of the agreement. Actuate software products are protected by U.S. and International patents and patents pending. For a current list of patents, please see <http://www.actuate.com/patents>.

Actuate Corporation trademarks and registered trademarks include:

Actuate, ActuateOne, the Actuate logo, Archived Data Analytics, BIRT, BIRT 360, BIRT Analytics, BIRT Data Analyzer, BIRT Performance Analytics, Collaborative Reporting Architecture, Dynamic Data Web, e.Analysis, e.Report, e.Reporting, e.Spreadsheet, Encyclopedia, Interactive Viewing, OnPerformance, Performancesoft, Performancesoft Track, Performancesoft Views, Quite4Me, Quiterian, Report Encyclopedia, Reportlet, The people behind BIRT, X2BIRT, and XML reports.

Actuate products may contain third-party products or technologies. Third-party trademarks or registered trademarks of their respective owners, companies, or organizations include:

Mark Adler and Jean-loup Gailly (www.zlib.net): zLib. Apache Software Foundation (www.apache.org): Axis2, log4, Tomcat. Boost.org: Boost libraries, licensed under the Boost Software License. CURL (curl.haxx.se): Curl, licensed under a MIT/X derivate license. International Components for Unicode (ICU): ICU library. Marcin Kalicinski (rapidxml.sourceforge.net): RapidXML, licensed under the Boost Software License. Bruno Lowagie and Paulo Soares: iTextSharp, licensed under the Mozilla Public License (MPL). Math.NET: Math.NET, licensed under the MIT/X11 License. Microsoft Corporation: Access Database Engine, SQL Server Express. opensv team (sourceforg.net): opensv. openssl.org: OpenSSL, licensed under the OpenSSL license. qooxdoo.org: qooxdoo, licensed under the Eclipse Public License (EPL). Dave Scriven (svg.codeplex.com): SVG Rendering Engine, licensed under the Microsoft Public License. SQLAPI: SQLAPI++. sqlite.org: SQLite, public domain. stlsoft.org: STLSoft libraries, licensed under the BSD license. Matthew Wilson and Garth Lancaster (www.pantheios.org): Pantheios, licensed under a modified BSD license.

All other brand or product names are trademarks or registered trademarks of their respective owners, companies, or organizations.

Document No. 150731-2-580301 September 28, 2015

Contents

About Administering BIRT Analytics	iii
---	------------

Part 1

Administering the BIRT Analytics system

Chapter 1

Using BIRT Analytics Administration	3
--	----------

About BIRT Analytics Administration	4
Accessing BIRT Analytics Administration	4
Understanding BIRT Analytics Administration	4
Checking the BIRT Analytics release	5
Configuring security	5
Managing security roles	6
Managing access permissions over database objects	8
Managing security filters	9
Security filter query syntax	9
Using multiple security filter queries	10
Security filter management	10
Managing profiles	11
Defining sensitive data	13
Synchronizing the application database	14
Removing temporary information	14
Defining password policy	15
Configuring users and groups	16
Configuring users	16
Configuring groups	17
Configuring the user repository	19
Using the BIRT Analytics repository	19
Using a BIRT iHub user repository	19
Using an Active Directory user repository	20
Mapping user profiles to the external user repository	21
Resetting the user repository settings	22
Configuring system options	22
Managing map images	22
Managing report styles	23
Configuring the e-mail server	24
Monitoring use	25
Managing connections	25
Viewing temporary file usage	26
Viewing usage statistics	26

Chapter 2

Configuring BIRT Analytics	29
---	-----------

About the configuration files	30
Configuring BIRT Analytics Application	30
Configuring BIRT Analytics Administration	31
Configuring BIRT Analytics Client	33
Configuring BIRT Analytics Loader	35
Configuring BIRT Analytics connectors	36

Configuring BIRT Analytics REST API	36
Configuring BIRT Analytics FastDB	37

Part 2

Administering BIRT Analytics reference

Chapter 3

Administering BIRT Analytics functional reference	45
Administering BIRT Analytics functional reference	46
General	46
Administration	48
Administration	48
Access control list (ACL)	49
Configuration	50
Folders	50
Functionalities	50
Groups	51
Integrity	51
Profile	52
Roles	52
Users	52
Analysis	53
Analysis	53
Bubble diagram	54
Calculate Pareto	54
Crosstab	54
Evolution diagram	54
Gallery	55
Map diagram	55
Profile	55
Venn diagram	56
Data exploration	56
Engine security	57
Engineering	57
Engineering	57
Edit engineering fields	58
Events and Alerts	59
Actions	60
Import-Export	61
Links	63
Plug-ins	63
Plug-ins	63
Cworkflow	63
Campaign management	64
Campaign planning	65
Configure CWorkflow	66
Events and Alerts	67
Data Mining	68
Algorithms	68
Preferences	69
Statistics	70

A b o u t A d m i n i s t e r i n g B I R T A n a l y t i c s

Administering BIRT Analytics includes the following chapters:

- *About Administering BIRT Analytics.* Provides an overview of this book.
- *Part 1. Administering the BIRT Analytics system.* Describes the general features of the BIRT Analytics Administration application and related operational tasks.
- *Chapter 1. Using BIRT Analytics Administration.* Describes BIRT Analytics administration modules, such as security, users, groups, configuration, and monitoring.
- *Chapter 2. Configuring BIRT Analytics.* Describes the configuration files used by the different applications in the BIRT Analytics system.
- *Part 2. Administering BIRT Analytics reference.* Provides reference information on BIRT Analytics administration modules and terminology.
- *Chapter 3. Administering BIRT Analytics functional reference.* Describes the functionalities that the administrator uses to configure permissions in the security role management module in BIRT Analytics Administration.

Part One

Administering the BIRT Analytics system

- Using BIRT Analytics Administration
- Configuring BIRT Analytics

1

Using BIRT Analytics Administration

This chapter contains the following topics:

- About BIRT Analytics Administration
- Configuring security
- Configuring users and groups
- Configuring system options
- Monitoring use

About BIRT Analytics Administration

The following sections describe the modules available in the BIRT Analytics Administration application and provide information on how to configure the system.

Accessing BIRT Analytics Administration

BIRT Analytics Administration runs as a browser-based application. After installation, the administrator opens a browser and connects to the administration application by typing a URL of the following format:

```
http://bahost:8110/baadmin
```

bahost is the name of the system on which BIRT Analytics Administration is deployed.

8110 is the port number used by BIRT Analytics.

baadmin is the context for BIRT Analytics Administration.

On initial access, the administrator logs in to the application by typing the user name, Administrator, and the default password, PASSWORD, as shown in Figure 1-1. The administrative user, Administrator, has full permission to modify all configurable features of the BIRT Analytics system.

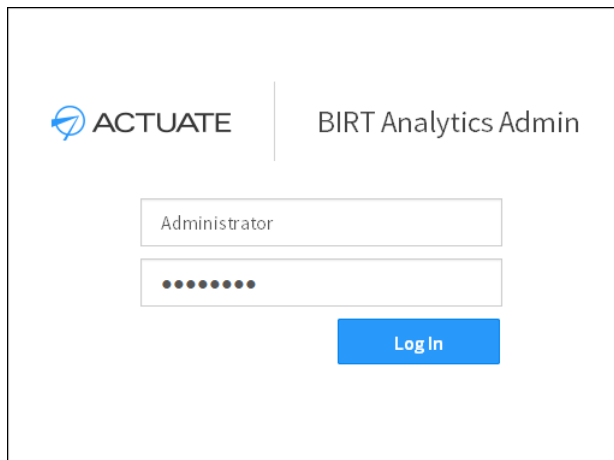


Figure 1-1 BIRT Analytics Administration login

Actuate recommends changing the administrator password immediately after accessing the system to maintain security. For security reasons, Actuate also recommends that all users, including the administrator, log out of the system before closing any BIRT Analytics application. To log out, choose Logout in the top banner menu, as shown in Figure 1-2.

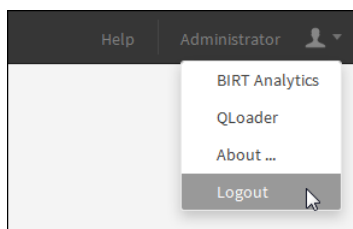


Figure 1-2 Logout menu option

Understanding BIRT Analytics Administration

The main options list in the BIRT Analytics Administration application contains the following modules, as shown in Figure 1-3:

- **Security**
Manage a security role, access control list (ACL), security filter, profile, sensitive data definition, database synchronization, temporary file information, and password policies.
- **User management**
Create, modify, or delete a user account. Create, modify, or delete a group. A group is a set of users belonging to the same organizational unit who share the same permissions for performing tasks. Set up the user repository.
- **Configuration**
Configure settings used in document generation, such as map management and report styles, and Simple Mail Transfer Protocol (SMTP) e-mail transmission.
- **Monitoring use**
Manage connections, track disk usage for temporary files, and monitor use of the BIRT Analytics tool on database objects.

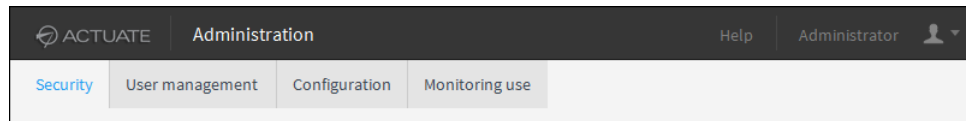


Figure 1-3 BIRT Analytics Administration modules

Checking the BIRT Analytics release

To find the release number of the BIRT Analytics applications, choose About in the top banner menu, as shown in Figure 1-4.

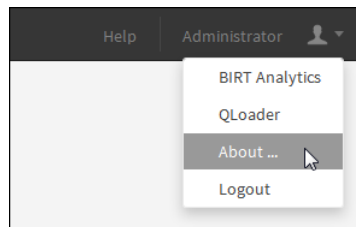


Figure 1-4 About menu option

The release information appears, as shown in Figure 1-5.

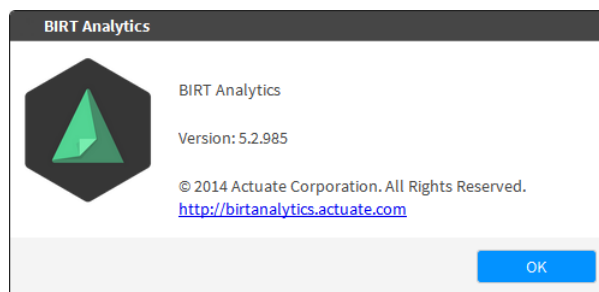


Figure 1-5 BIRT Analytics release information

Configuring security

The Security pages allow the administrator to manage security roles, access to objects, specify security filters, define password policies, browse logs, synchronize the database, specify password policies, and perform other security maintenance actions.

BIRT Analytics Administration provides the following security pages, as shown in Figure 1-6:

- **Security role management**
Create, modify, or delete a security role and configure permissions in the BIRT Analytics system.
- **Access permissions on objects**
Create, modify, or delete a security group or access control list (ACL), and manage privileges over database objects.
- **Security filters**
Create, modify, or delete a security filter to limit the access to data stored in a database.
- **Profiles**
Create, modify, or delete a profile, which is a set of roles, security groups, and security filters assigned to a user.
- **Define sensitive data**
Specify sensitive data columns for audit.
- **Synchronize**
Synchronize the application database with the BIRT Analytics Engine repository.
- **Remove temporary information**
Remove all temporary files and records used by the application.
- **Password policies**
Define the rules to use in specifying a user password.

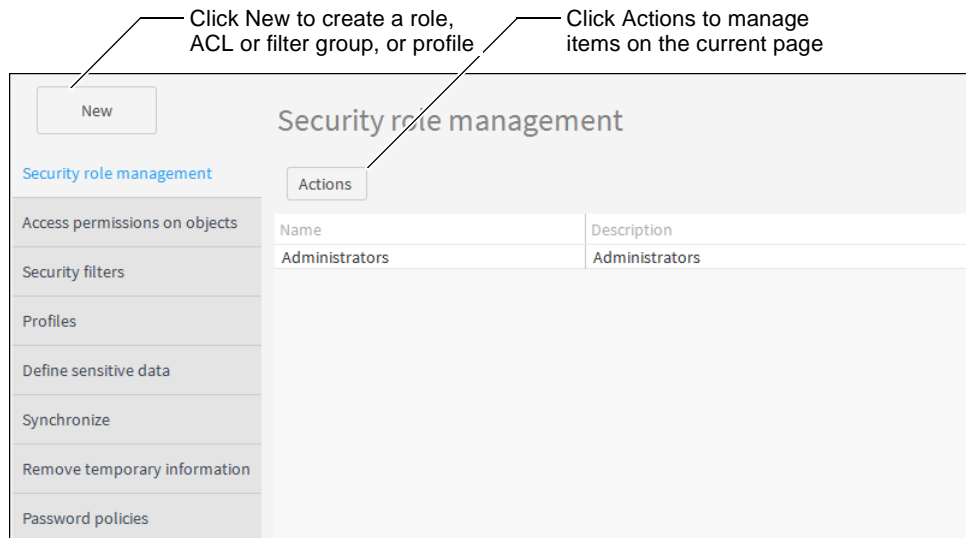


Figure 1-6 BIRT Analytics security options

The following sections provide more information on these security options.

Managing security roles

A security role defines the actions that a user can perform on accessible data.

The Security role management page allows the administrator to create, modify, or delete a security role. Clicking Actions provides the following choices:

- **Refresh**
Choose Refresh to update the list of roles. Any changes that another administrator made to the roles available are displayed.
- **New**
Choose New to define a new role. In New role, type the role name and a description, and select the functionalities to grant to the role. In Functionalities, select the triangle to expand a functional category. Select the higher-level category to include all elements, or select individual elements in the category list to configure a more restricted subset of privileges, as shown in Figure 1-7.

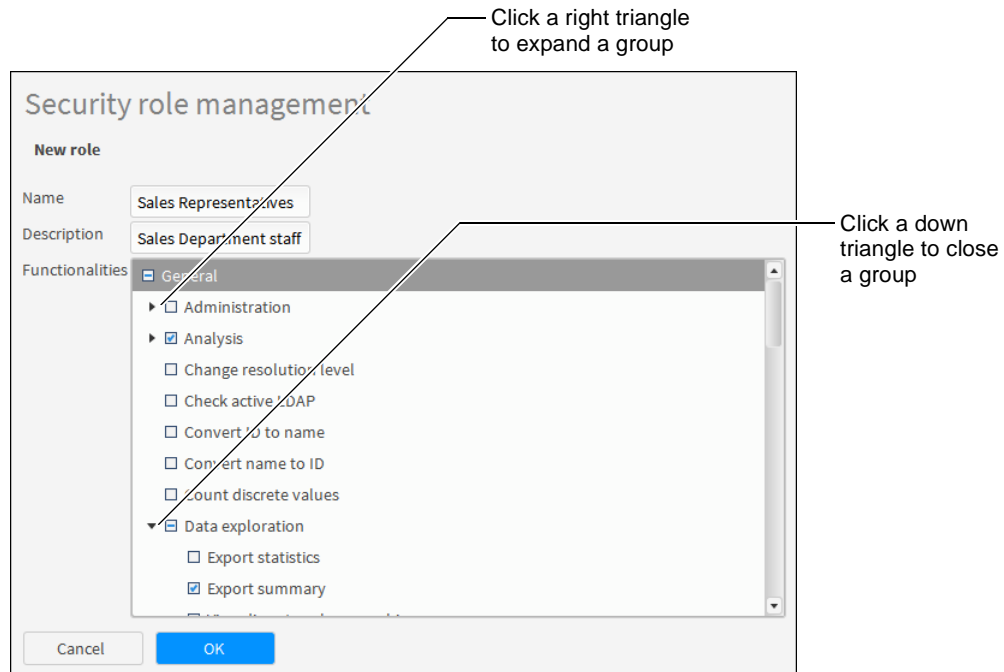


Figure 1-7 Creating a role

Choose OK. The new role appears in the list of security roles.

- **Modify**
In the list of roles, select a role. Then, click Actions and choose Modify to change the settings specified for the role. In Updating role, update the role name or description, select any additional functionalities or privileges to grant to the role, or remove a functionalities selection to remove from the role. For example, after upgrading a license to support a new plug-in, such as Campaign Workflow (Cworkflow), enable the module by assigning the functionality to a security role.
Choose OK.
- **Create As**
In the list of roles, select a role. Then, click Actions and choose Create As to define a new role containing the settings specified for the selected role. Create As copies the functionalities for the selected role to the new role definition. In Create As, type the role name and a description. Then, select any additional functionalities to grant to the new role. Deselect functionalities to remove from the new role.
Choose OK. The new role appears in the list of security roles.

- Delete
In the list of roles, select a role. Then, click Actions and choose Delete to remove a role. In Deleting role, the name, description, and list of functionalities appears.
Choose OK. A prompt appears. Choose Yes to confirm deleting the role.

Managing access permissions over database objects

Access permissions restrict a user's data access to a particular set of databases, tables, or columns. A set of access permissions defines a security group.

The Access permissions on objects page allows the administrator to create, modify, or delete a security group and manage privileges for database objects. Clicking Actions provides the following choices:

- Refresh
Choose Refresh to update the list of groups. Any changes that another administrator made to the groups available are displayed.
- New
Choose New to define a new group. In New group, type the group name and a description, as shown in Figure 1-8.

The screenshot shows a dialog box titled "Access permissions on objects" with a "New group" tab. It contains two text input fields: "Name" with the value "Data Architect" and "Description" with the value "Warehouse designer". Below these is a checked checkbox with the text "Updates occur immediately. Ask for confirmation before applying changes?". To the right of this checkbox is a "Go up a level" button. Underneath is a table with the following structure:

Object	All	None	Custom
	All	None	Custom

At the bottom of the dialog are "Cancel" and "OK" buttons.

Figure 1-8 Creating a group

Choose OK. The new group appears in the list of security groups.

To define access to database objects for the new group, click Actions and choose Modify.

- Modify
In the list of groups, select a group. Then, click Actions and choose Modify to change the settings for the group. In Updating group, type a new group name or description and grant access to database objects by choosing All, None, or Custom. An object is either a database or a table or field in the database hierarchy.

When *Ask for confirmation before applying changes?* is not selected, no confirmation message appears before the updated settings are applied.

Choose All to grant full access to the selected object and all objects in that object.

Choose None, the default setting, to restrict access to the selected object and all objects in that object.

Choose Custom to specify limited access to individual database tables and columns. The objects that make up the selected object appear. Choose All or None for each object, as shown in Figure 1-9.

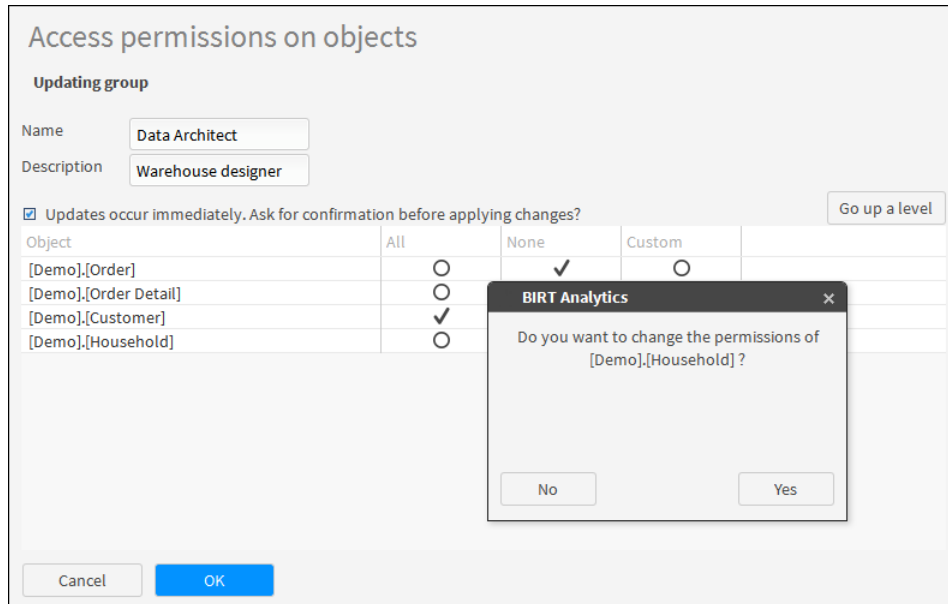


Figure 1-9 Modifying the access for a group

Choose OK. Changes to the group name and description appear in the list of groups. If Updates occur immediately is not selected, the updated access settings are applied now.

- **Create As**

In the list of groups, select a group. Then, click Actions and choose Create As to define a new group containing the settings, including the name, description, and list of data objects specified for the selected group. Create As copies the settings defined for the selected group to the new group definition. In Create As, type the group name and a description.

Choose OK. The new group appears in the list of security groups.

To define access to database objects for the new group, click Actions and choose Modify.

- **Delete**

In the list of groups, select a group. Then, click Actions and choose Delete to remove a group. In Deleting group, the name, description, and list of data objects appears.

Choose OK. A prompt appears. Choose Yes to confirm deleting the group.

Managing security filters

A security filter restricts the set of data values that a named group of users can read from a database. A security filter is made up of one or more queries.

Security filter query syntax

A security filter query is a comparison of a column and data value, as shown in the following example:

```
[Demo].[Household].[Town] EQ Big Bear Lake
```

The query must conform to the following syntactical rules:

- Object names, such as columns and tables, are case sensitive.

- The set of available operators is:
EQ, NE, GE, GT, LE, LT
- A string value does not require quotation mark delimiters (" or ').

Using multiple security filter queries

A security filter supports multiple queries. The filter joins queries using a logical AND if a link exists in the repository between the queries. If the repository does not provide a link between the queries, the filter joins the queries using a logical OR. For example, the following two queries in a security filter:

```
[Demo].[Household].[Town] EQ Brisbane
[Demo].[Customer].[Gender] EQ F
```

are equivalent to:

```
([Demo].[Household].[Town] EQ Brisbane)
AND
([Demo].[Customer].[Gender] EQ F)
```

The following two queries that have no link in the repository:

```
[FS].[Customer].[Occupation] EQ Director
[Demo].[Customer].[Gender] EQ F
```

are equivalent to:

```
([FS].[Customer].[Occupation] EQ Director)
OR
([Demo].[Customer].[Gender] EQ F)
```

Security filter management

The Security filters page allows the administrator to create, modify, or delete a security filter and specify one or more queries to control access to data.

Clicking Actions provides the following choices:

- Refresh
Choose Refresh to update the list of security filters. Any changes that another administrator made to the security filters available are displayed.
- New
Choose New to define a new security filter. In New security filter group, type the name and a description. Then, choose New and type a query. Choose Test query to validate the query. If valid, the application displays the records obtained, as shown in Figure 1-10. Choose OK to add the query. The query appears in the list of queries for the security filter.
Repeat the procedure to add a query if the security filter requires more queries.
Choose OK. BIRT Analytics revalidates the queries. If any query contains an error, BIRT Analytics does not save the security filter. Correct the error and choose OK again. The security filter appears in the list of filters.

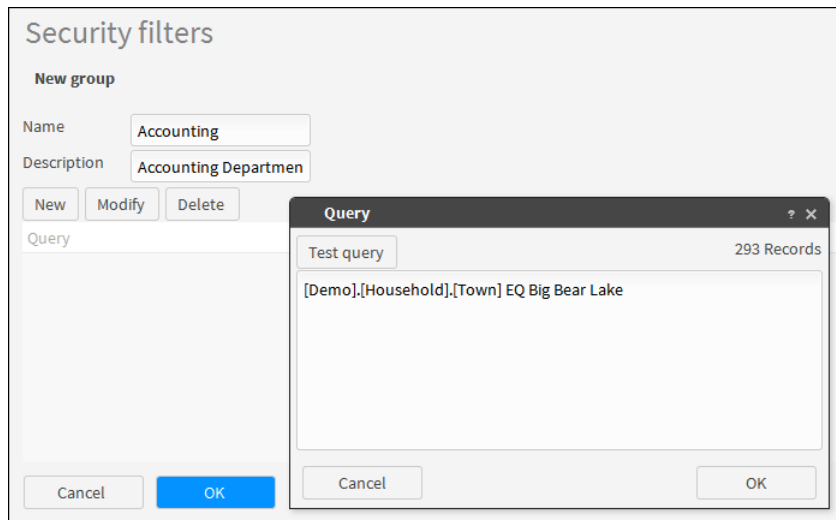


Figure 1-10 Creating a security filter

- **Modify**

In the list of security filters, select a security filter. Then, click Actions and choose Modify to change the settings for the filter. In Updating group, type the name and a description. To add a new query to the filter, choose New. To modify or delete a query, select the query. Then choose Modify or Delete.

Choose Test query to validate the query. If valid, the application displays the records obtained. Choose OK to add the query. The query appears in the list of queries for the security filter. Choose OK to update the security filter.

- **Create As**

In the list of security filters, select a security filter. Then, click Actions and choose Create As to define a new filter containing the settings specified for the selected filter. In Create as, type the name and a description for the new filter. To add a new query to the filter, choose New. To modify or delete a query, select the query. Then choose Modify or Delete.

Choose Test query to validate each new or modified query. If valid, the application displays the records obtained and adds the query. Choose OK. The security filter appears in the list of current filters.

- **Delete**

In the list of security filters, select a security filter. Then, click Actions and choose Delete to remove a security filter. In Deleting group, the name, description, and filter queries appear.

Choose OK. A prompt appears. Choose Yes to confirm deleting the filter.

Managing profiles

A profile combines one or more security roles, security filters, security groups, and users into a matrix that defines the items that a user can access. To log in to BIRT Analytics, a user must be assigned to a profile.

The Profiles page allows the administrator to create, modify, or delete a profile, and select roles, security groups, security filters, and users to add to the profile. Clicking Actions provides the following choices:

- **Refresh**
Choose Refresh to update the list of profiles. Any changes that another administrator made to the profiles available are displayed.
- **New**
Choose New to define a new profile. In New profile, type the profile name and a description. Then, select the roles, security groups, security filters, and users to add to the profile, as shown in Figure 1-11.

If BIRT Analytics security uses an LDAP server, LDAP groups also appear. If the LDAP groups are visible, the administrator can link the profile to a group defined in the LDAP server. If a user belongs to an LDAP group, the BIRT Analytics user inherits the privileges and restrictions from the LDAP group profile. When using LDAP, it is not necessary to select users as the list of users is linked to the LDAP group.

Choose OK. The profile appears in the list of profiles.

The screenshot shows a 'Profiles' dialog box with the following elements:

- Title:** Profiles
- Section:** New profile
- Name:** Text box containing 'Sales'
- Description:** Text box containing 'Sales Department user'
- User repository groups:** A dropdown menu with a downward arrow.
- Roles:** A list box containing 'Administrators', 'Sales Managers', and 'Sales Representatives'. 'Sales Managers' and 'Sales Representatives' are highlighted.
- Security groups:** A list box containing 'Data Architect', 'Master users', and 'Sales'. 'Sales' is highlighted.
- Security filters:** A list box containing 'Accounting' and 'Sales'. 'Sales' is highlighted.
- Users:** A list box containing 'Administrator' and 'Sales SVP'. 'Sales SVP' is highlighted.
- Buttons:** 'Cancel' and 'OK' buttons at the bottom.

Annotations on the right side of the dialog:

- Line pointing to 'User repository groups': LDAP groups appear in this list
- Line pointing to 'Data Architect': A non-highlighted item is not included in the profile
- Line pointing to 'Sales SVP': A highlighted item is included in the profile

Figure 1-11 Creating a profile

- **Modify**
In the list of profiles, select a profile. Then, click Actions and choose Modify to change the settings specified for the profile. In Updating profile, update the name and description. Select any additional roles, security groups, security filters, or users to add to the profile, or remove these items from the profile.
Choose OK.
- **Create As**
In the list of profiles, select a profile. Then, click Actions and choose Create As to define a new profile containing the settings specified for the selected profile. In New profile as, type the profile name and a description. Then, select the roles, security groups, security filters, and users to add to the profile.
Choose OK. The profile appears in the list of profiles.
- **Delete**
In Current profiles, select a profile. Then, click Actions and choose Delete to remove a profile. In Deleting profile, the name, description, and list of roles, security groups, security filters, or users appear.
Choose OK. A prompt appears. Choose Yes to confirm deleting the profile.

Defining sensitive data

Sensitive data are columns for which BIRT Analytics audits all access.

The Sensitive data page allows the administrator to specify which data to audit when tracking user read and update activities. Audit tracking records the following information:

- User who accessed the data
- Date and time the access occurred
- Data read or updated

To specify data for audit, select the following:

- Databases
- Tables
- Columns

The information is recorded in a log file, by default in:

[Installation folder]\BIRTAnalytics\log\electronsensitive.log

In the list of columns, select one or more columns and choose Add to list to move the columns to the list of sensitive columns. In the list of sensitive columns, select one or more columns and choose Remove from list to move a column out of the list of sensitive columns, as shown in Figure 1-12.

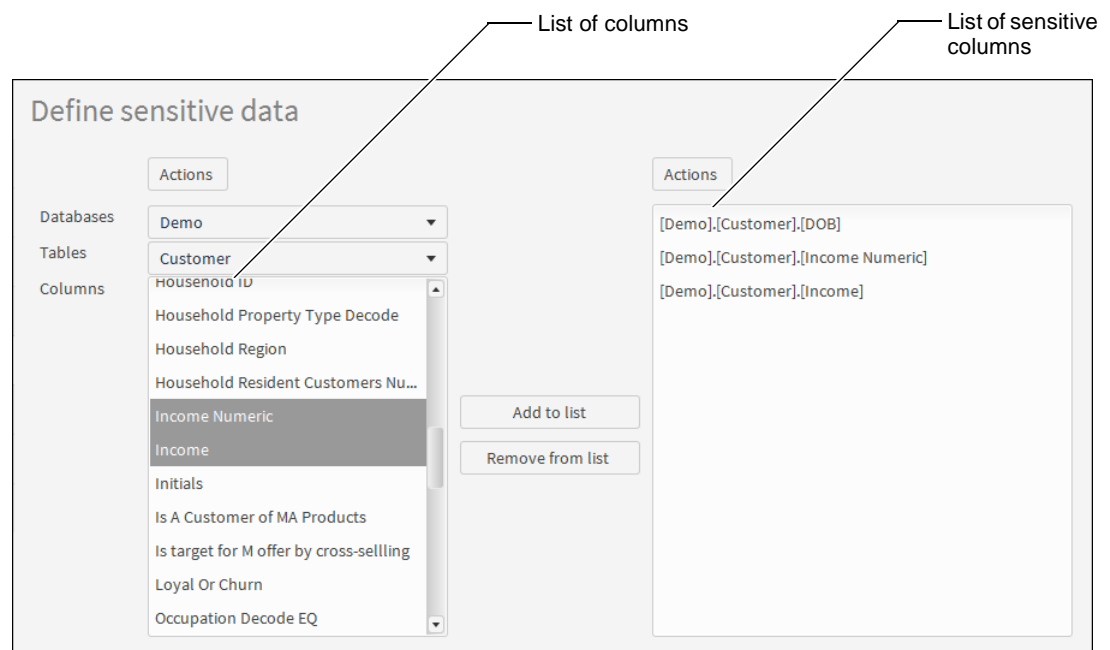


Figure 1-12 Specifying sensitive data

Each list of columns has an Actions button. Clicking the button provides the following commands:

- Refresh
Choose Refresh to update the list of columns. Any changes that another administrator made to the definitions of sensitive columns are displayed.
- Select all
Choose Select all to select all columns in the list. Then, choose Add to list or Remove from list to make all columns in a table sensitive or not sensitive.

- Deselect all
Choose Deselect all to remove the selection from all columns in the list. Use this command if you need to discard your selections and start over.

Synchronizing the application database

The Synchronize page allows the administrator to update the application database to contain the most recent changes in the BIRT Analytics Engine repository. Execute this option after making a change in the analytical repository that alters the database structure, such as the addition, modification, or deletion of a column, table, or other data object.

The Synchronize page displays the following warning:

WARNING: The synchronization process deletes the database and replaces it with the database structure in the Engine. All outdated links between security groups and objects are removed.

Choose OK to update the application database with the BIRT Analytics Engine repository, as shown in Figure 1-13. A progress animation appears while the synchronization takes place.

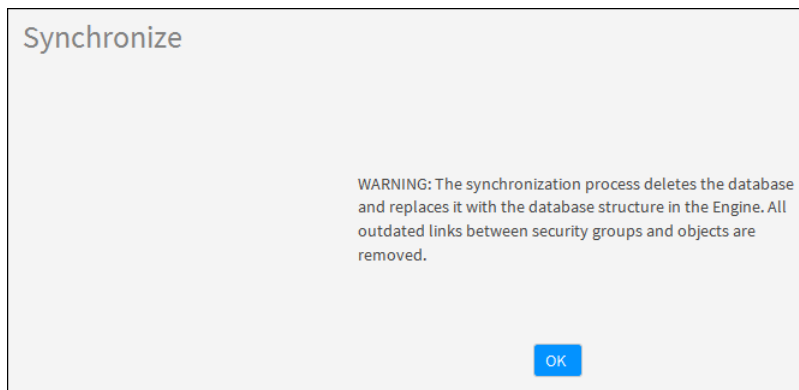


Figure 1-13 Synchronizing the application database

Removing temporary information

A temporary file is a temporary data file generated by the BIRT Analytics application. The Remove temporary information page allows the administrator to remove all temporary files and records used by the application to return disk and memory resources to the system. Use this option to refresh the cache after performing analytical calculations that contain obsolete data.

The Remove temporary information page displays the following warning:

WARNING: This process will remove all temporary files and records used by the application. This action may affect any users who are working in BIRT Analytics right now.

Choose OK to remove all temporary files and records used by the application, as shown in Figure 1-14. A progress animation appears while BIRT Analytics removes the temporary information.

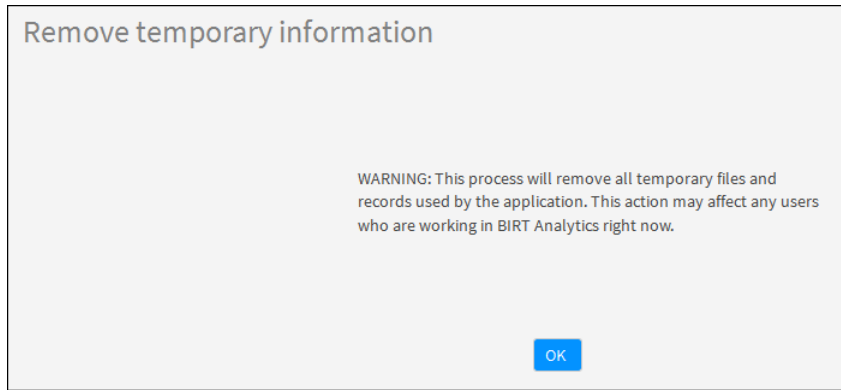


Figure 1-14 Removing temporary information

Defining password policy

The Password policies page allows the administrator to define rules to use in specifying a user password. The following choices are available, as shown in Figure 1-15:

Select any of the following items to define password policies:

- It must contain at least one lowercase letter
- It must contain at least one uppercase letter
- It must include at least one of these characters
_ , - , ! , . , \$, % , (,) , = , | , @ , # , € , * , ~ , " , " , . , " "
- It must include at least one number
- Password length has to be greater than 6 characters
- Password length has to be greater than 8 characters
- Password length has to be greater than 10 characters

Click Actions and choose Save to implement the password policy changes.

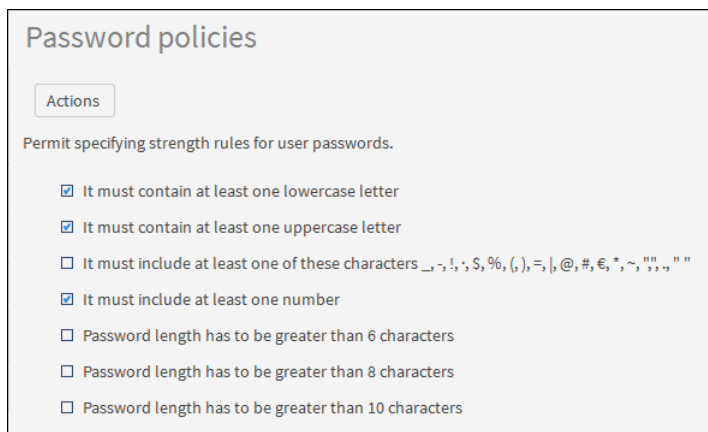


Figure 1-15 Configuring password policies

To see any changes that another administrator made to the password policies, click Actions and choose Refresh.

Configuring users and groups

The User management pages allow the administrator to manage user accounts, user groups, and connection to an Active Directory user repository. If the system security is integrated with an Active Directory system, managing users and groups in the BIRT Analytics Administration application does not change the configuration of the corresponding objects.

A user cannot log in to BIRT Analytics unless the account is assigned to a profile. For information about profiles, see “Managing profiles.”

BIRT Analytics Administration provides the following user and group configuration pages:

- **User management**
Create, modify, or delete a user account.
- **Group management**
Create, modify, or delete a user group.
- **User repository**
Specify the repository used for user authentication.

Configuring users

The User management page allows the administrator to create, modify, or delete a user account. Clicking Actions provides the following choices:

- **Refresh**
Choose Refresh to update the list of user accounts. Any changes that another administrator made to the users available are displayed.
- **New**
Choose New to define a new user. In Create, specify the settings shown in Table 1-1, as shown in Figure 1-16.

Table 1-1 User definition settings

Setting	Purpose and value
Login	Unique user ID.
Password	Password that conforms to password policies specifications.
Name	User name.
Language	Local language settings specified for the BIRT Analytics application environment.
Theme	Presentation theme specified for the user application.
User type	ADMIN or POWER user type.
Expiration date	Whether the user account becomes inactive at a set date and the date on which to deactivate user account.
Active	If selected, the user account is active. If deselected, the user account is inactive although the user configuration remains on the system.
Must change password at next login	Whether the user must change password at the next login.
Email	User e-mail address.

Figure 1-16 Creating a user

Choose OK. The user appears in the list of users.

- **Modify**

In the list of users, select a user. Then, click Actions and choose Modify to change the settings specified for the user. In Modify, update any of the settings shown in Table 1-1.

Choose OK.

- **Create as**

In the list of users, select a user. Then, click Actions and choose Create as to define a new user account containing the settings specified for the selected user. In Create as, type new values for Login and Name. Then, update any of the other settings shown in Table 1-1.

Choose OK. The user appears in the list of users.

- **Delete**

In the list of users, select a user. Then, click Actions and choose Delete to remove the user. In Delete, the settings for the selected user appear.

Choose OK. A prompt appears. Choose Yes to confirm deleting the user.

Configuring groups

The Groups management page allows the administrator to create, modify, or delete a group. This option provides the following choices:

- **Refresh**

Choose Refresh to update the list of user groups. Any changes that another administrator made to the user groups available are displayed.

- **New**

Choose New to define a new group. In Create, specify the settings shown in Table 1-2, as shown in Figure 1-17.

Table 1-2 User group definition settings

Setting	Purpose and value
Name	User group name.
Description	Description of group function or purpose.

Table 1-2 User group definition settings

Setting	Purpose and value
Users	List of BIRT Analytics users. Select any user in the Users list to add to the group.

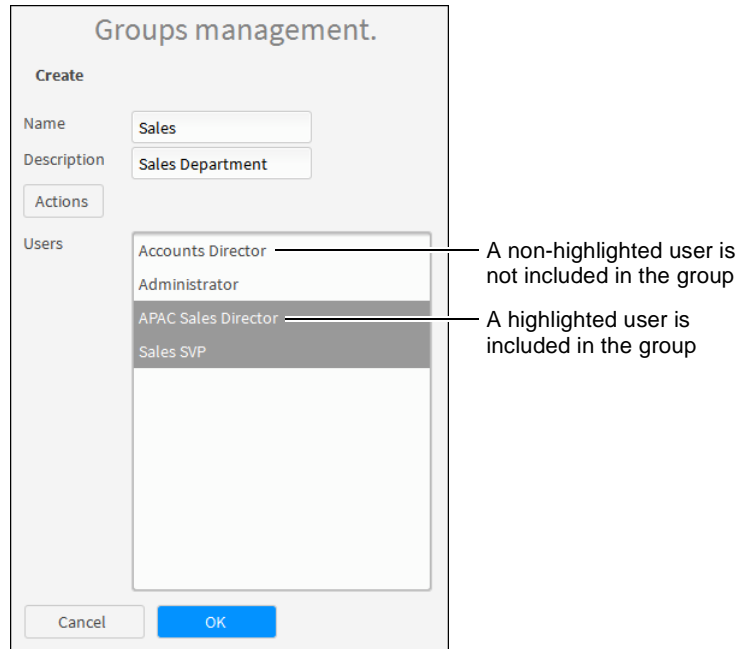


Figure 1-17 Creating a BIRT Analytics user group

The list of users has an Actions button. Clicking the button provides the following commands:

- Refresh
Choose Refresh to update the list of users. Any changes that another administrator made to the set of users are displayed.
- Select all
Choose Select all to select all users in the list.
- Deselect all
Choose Deselect all to remove the selection from all users in the list. Use this command if you need to discard your selections and start over.

Choose OK. The user group appears in the list of user groups.

- Modify
In the list of groups, select a group. Then, click Actions and choose Modify to change the group settings specified for the group. In Modify, select any user in the Users list to add to the group or remove the selection from a user to remove them from the group.

Choose OK. The group appears in the list of user groups.

- Create as
In the list of user groups, select a group. Then, click Actions and choose Create as to define a new user group containing the settings specified for the selected user group. In Create as, type a new value for Name. Then, update any of the other settings shown in Table 1-2.

Choose OK. The user group appears in the list of user groups.

- **Delete**
In the list of groups, select a group. Then, click Actions and choose Delete. In Delete, the settings for the selected group appear.
Choose OK. A prompt appears. Choose Yes to confirm deleting the user group.

Configuring the user repository

The user repository defines and controls users and groups. The default user repository is BIRT Analytics built-in repository.

The user repository page enables the administrator to link the users and groups in the BIRT Analytics application to the default repository, to a BIRT iHub repository or to an Active Directory repository.

BIRT Analytics uses the credentials of the logged-in user to verify the connection to the specified repository. If the logged-in user credentials do not authenticate in the repository, BIRT Analytics does not change the user repository. This behavior ensures continued access to the BIRT Analytics applications.

Using the BIRT Analytics repository

As this is the default repository, BIRT Analytics security is already enabled the first time you open the User repository tab. If necessary, re-enable it. You can set the following property:

- **Expires in**
Selecting Expires makes it possible to limit the number of days that the user password will be valid by entering the desired days in the days field. The password must be reset each time the specified days have passed.

Using a BIRT iHub user repository

To set the user repository to a BIRT iHub volume, set the following properties as shown in Figure 1-18:

- **iHub security enabled**
Selecting iHub security enabled indicates that you will be using a BIRT iHub user repository and the following fields must be filled in:
 - **iHub Server**
A URL containing the fully qualified domain name of the machine running BIRT iHub and the port on which the server listens. The default port is 8000.
 - **Volume**
The volume on which to verify the user credentials. This name is case sensitive. The default volume created on BIRT iHub installation is Default Volume.

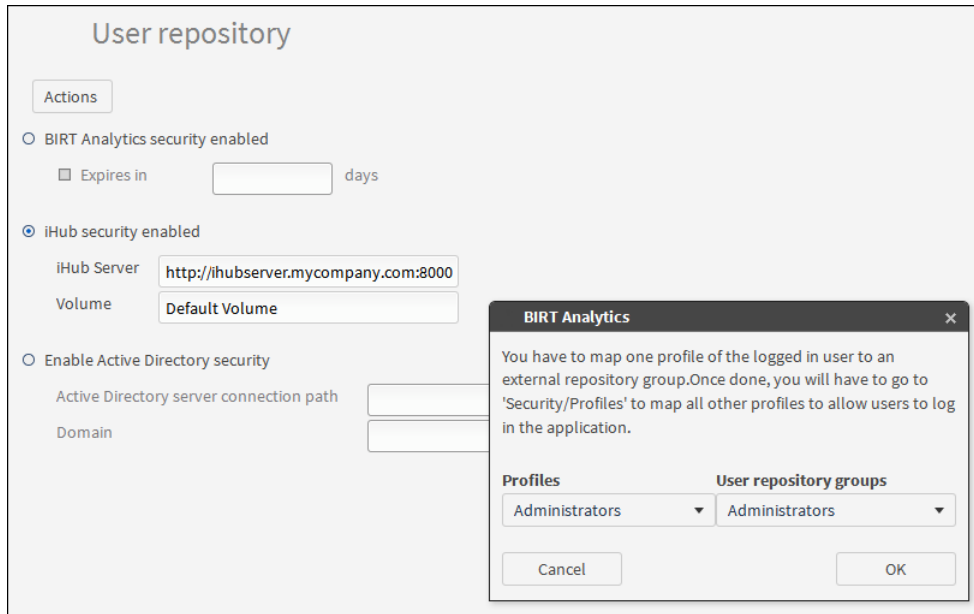


Figure 1-18 Configuring the BIRT iHub user repository

Click Actions and choose Save to save the user repository settings.

Map the Administrators profile to the matching user repository group. Choose OK.

You must now map the user profiles to the BIRT iHub groups. Failure to map the profiles prevents any user logins.

Using an Active Directory user repository

To set the user repository to an LDAP server, set the following properties, as shown in Figure 1-19. BIRT Analytics uses the system settings relating to the LDAP server for all other LDAP configuration values.

- Active Directory server connection path
The protocol and path to the Active Directory server and the port on which the server listens. Use either the network name of the server or the IP address. The protocol is LDAP:. The default port is 389.
- Domain
The network domain of the Active Directory server.

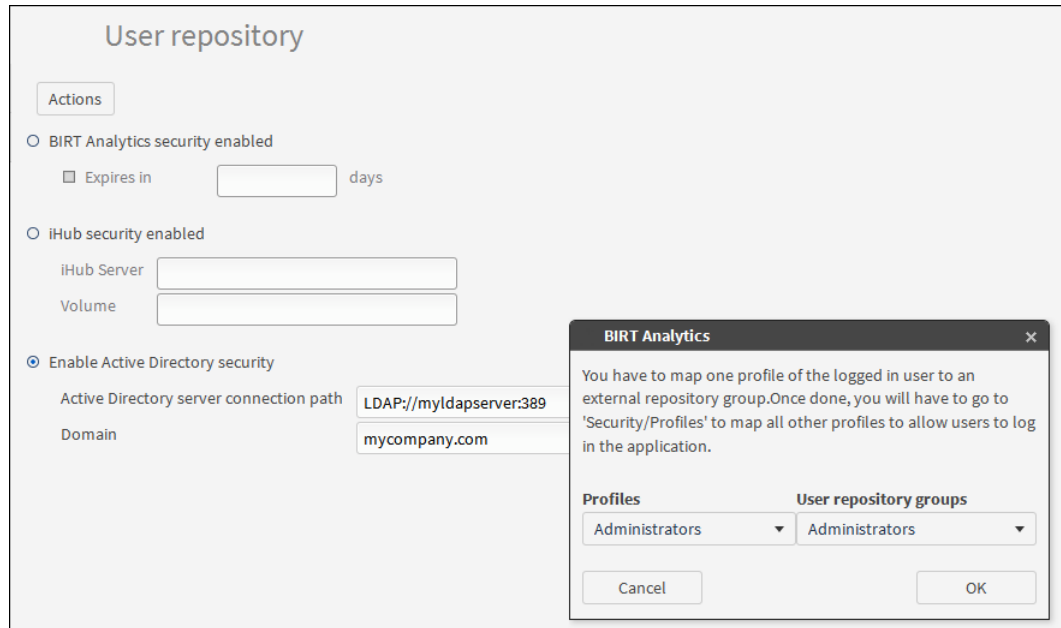


Figure 1-19 Setting an LDAP server as the user repository

Click Actions and choose Save to save the user repository settings.

Map the Administrators profile to the matching user repository group. Choose OK.

You must now map the user profiles to the LDAP groups. Failure to map the profiles prevents any user logins.

Mapping user profiles to the external user repository

To map user profiles to the external user repository, navigate to the Profiles page. For each profile, select the profile and choose Modify. Then, select a User repository group from the list, as shown in Figure 1-20.

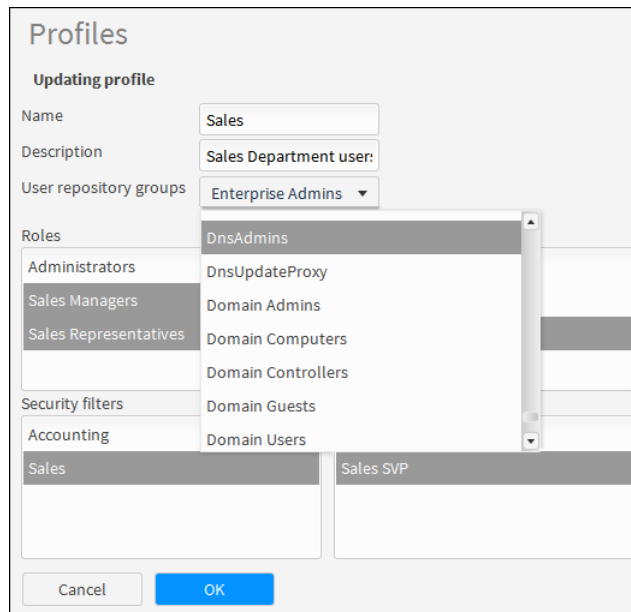


Figure 1-20 Selecting a group from the external user repository

Choose OK.

Resetting the user repository settings

Click Actions and choose Refresh to reset the display to the current user repository settings or to see changes that another administrator made to the user repository settings. BIRT Analytics discards unsaved changes and displays the current user repository settings.

Configuring system options

The Configuration pages allow the administrator to specify settings used in document generation, such as map management and report styles, and SMTP e-mail transmission.

BIRT Analytics Administration provides the following system configuration pages:

- Map management
Manage SVG files used by maps in BIRT Analytics.
- Styles admin
Manage Rich Text Format (RTF) styles for reports generated by BIRT Analytics.
- Configure SMTP server
Specify the Simple Mail Transfer Protocol (SMTP) configuration used for sending e-mail notifications.

Managing map images

The Map management page allows the administrator to upload, explore, or delete a Scalable Vector Graphics (SVG) map. This module allows the administrator to manage server folders that provide reference maps in the analysis module. Clicking Actions provides the following choices:

- Refresh
Choose Refresh to update the list of SVG map files. Any changes that another administrator made to the SVG files available are displayed.
- Upload SVG
Choose Upload SVG to upload one or more SVG map files to the BIRT Analytics system. In the prompt that appears, choose Upload SVG. Navigate to the folder containing SVG map files. Select one or more SVG map files, and choose Open. The map management module verifies that the file is an SVG file. If a file is a valid SVG file, the file name appears in the list of SVG files.
- Explore
In the list of SVG files, select a file. Then, click Actions and choose Explore to view the image. The SVG image appears in Explore SVG, as shown in Figure 1-21. This option only allows the administrator to view an image, not modify the file specification.

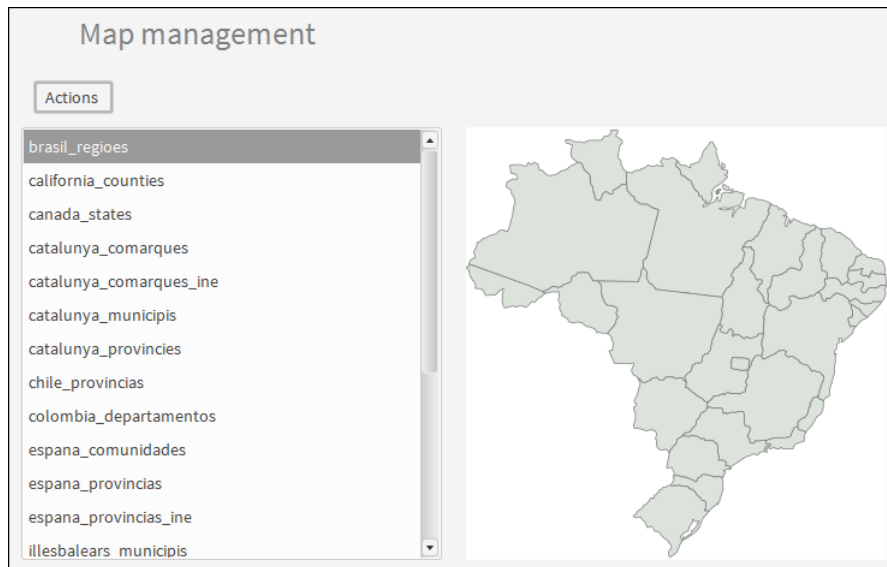


Figure 1-21 Exploring a map

- **Delete**
In the list of SVG files, select a file. Then, click Actions and choose Delete to remove the map.
Choose OK. A prompt appears. Choose Yes to confirm deleting the map from the list of SVG files.

Managing report styles

The Styles admin page allows the administrator to manage Rich Text Format (RTF) styles for reports generated by the BIRT Analytics tool. This page provides the following settings, as shown in Figure 1-22:

- **Title**
Select Font to specify a font, such as Arial or Verdana. Type a numeric value in Size to specify the size for report title text.
- **Body**
Select Font to specify a font, such as Arial or Verdana. Type a numeric value in Size to specify the size for report body text.
- **Margins**
Type numeric values in Left, Right, Top, and Bottom to specify the margin settings in pixels for report content.
- **Header**
Choose Upload picture to add an image to the report header. In the prompt that appears, choose Upload picture. The image file must be in either PNG or JPG format. Navigate to the image file, select it, and choose Open. The uploaded image file appears in the Header specification.

Styles admin

Actions

Use this option to manage report styles.

Title

Font: Source Sans Pro

Size: 18

Body

Font: Source Sans Pro

Size: 12

Margins

Left: 50

Right: 50

Top: 35

Bottom: 35

Header

Image: Upload picture

Figure 1-22 Managing style settings

Click Actions and choose Save to save the modified style settings.

Click Actions and choose Refresh to see changes that another administrator made to the styles.

Configuring the e-mail server

BIRT Analytics supports Simple Mail Transfer Protocol (SMTP) to send e-mail notifications.

The Configure SMTP server page allows the administrator to specify the settings for the SMTP server used for sending e-mail notifications. To configure an SMTP server, specify the following settings:

- **Server**
Name of the SMTP server
- **Port**
Port on which the SMTP server listens on the network
- **From**
E-mail account used to send the e-mail messages
- **User**
E-mail account user name
- **Password**
E-mail account password
- **Requires SSL**
Select to the security protocol used to send e-mails. The following values are available:

- Plain: E-mails do not use encryption.
- SSL: The SMTP service uses Secure Sockets Layer (SSL) to encrypt e-mails.
- TLS: The SMTP service uses Transport Layer Security (TLS) to encrypt e-mails.

Figure 1-23 shows a typical configuration.

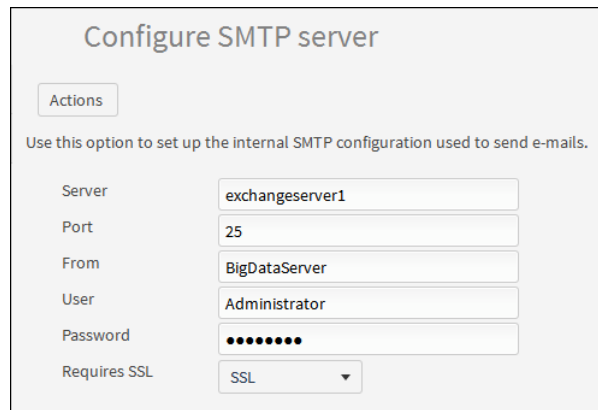


Figure 1-23 Configuring SMTP server settings

Click Actions and choose Save to save the SMTP server settings.

Click Actions and choose Refresh to see changes that another administrator made to the SMTP server settings.

Monitoring use

The Monitoring use pages allow the administrator to manage a connection, track disk usage for temporary files, and monitor use of the BIRT Analytics tool on database objects,.

BIRT Analytics Administration provides the following system configuration pages:

- Connection management
View the connections to the FastDB database used by BIRT Analytics.
- Temporary files
View the temporary file storage on disk used by BIRT Analytics.
- Statistics of use
View the usage of database fields by BIRT Analytics users.

Managing connections

The Connection management page allows the administrator to monitor the state of servers and connections, as shown in Figure 1-24. The server and connection icons indicate whether a component is running or paused.

Click Actions and choose Refresh to update the connection information.

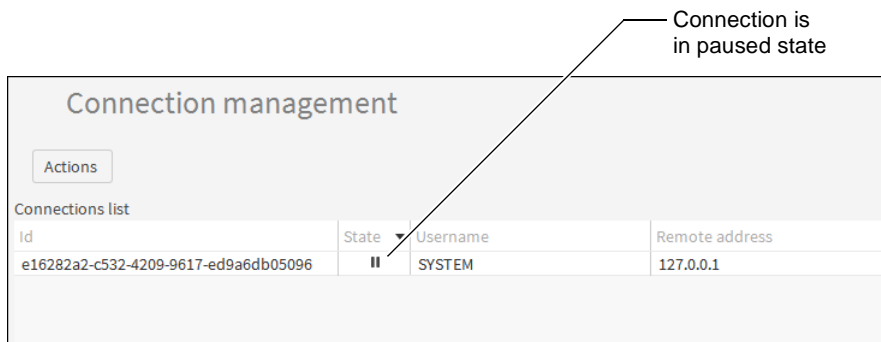


Figure 1-24 Viewing monitoring servers and connections

Viewing temporary file usage

The Temporary files page provides the following information on the disk space used by temporary files on all servers, as shown in Figure 1-25:

- Temp folder
File space used for analytical calculations
- Import folder
File space used during data import operations
- Export folder
File space used during data export operations

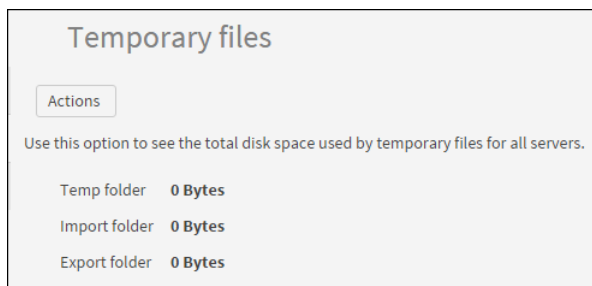


Figure 1-25 Viewing temporary files server and folder lists

Click Actions and choose Refresh to update temporary file information.

Viewing usage statistics

The Statistics of use page provides information on data column use. The administrator can use these statistics to determine which data columns have the highest and lowest access rates and use that information to optimize data queries. This page provides the following filters, as shown in Figure 1-26:

- Object
Searches only for actions performed on columns in which the object name contains the value in this field
- User
Searches only for actions performed by the specified user
- Start and End dates
Limits search to specified date range

- Actions performed on a column
 - Searches only for actions selected in the following category list:
 - Administration
 - Advanced Analysis
 - Analysis
 - Campaign Workflow
 - Direct exploration
 - Engineering
 - Import/Export
 - Indirect exploration
 - Links
 - Meta-information
 - Selections
 - Unknown

Choose Search to generate the statistics, displaying the object name and number of times the data has been accessed during the specified time range.

Choose Export to download the statistics to a comma-separated values (CSV) file.

The results of a query are sorted using the following conditions, as shown in Figure 1-26:

- Descending order of the actions performed on a column
- Ascending order of the name of the object

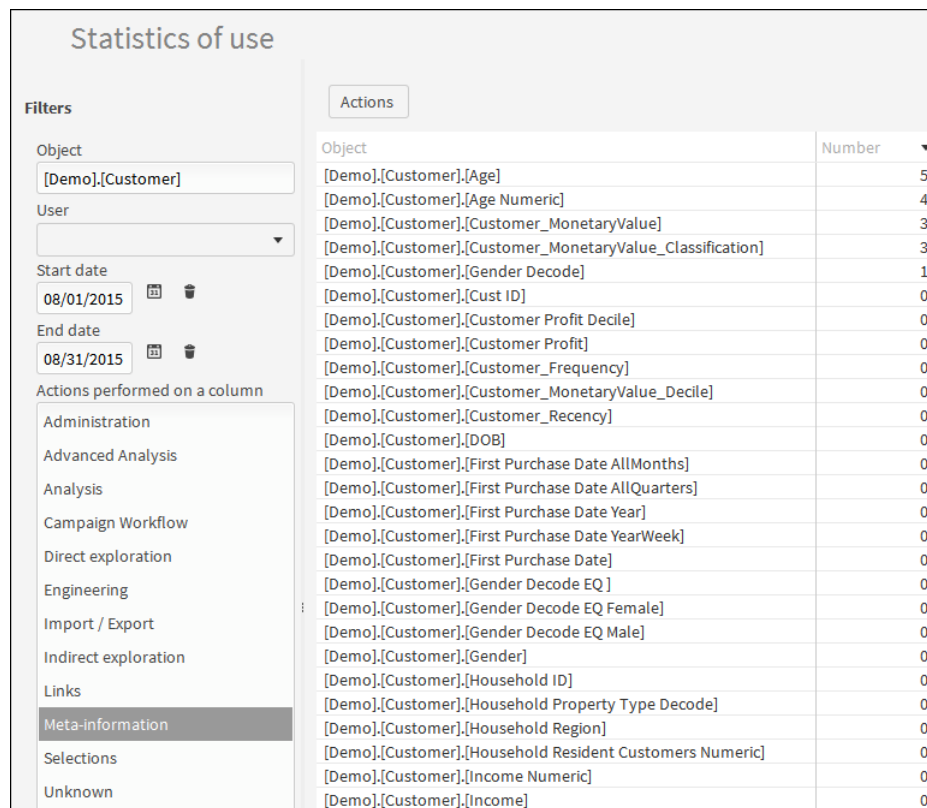


Figure 1-26 Viewing statistics using a filter

Configuring BIRT Analytics

This chapter contains the following topics:

- About the configuration files
- Configuring BIRT Analytics Application
- Configuring BIRT Analytics Administration
- Configuring BIRT Analytics Client
- Configuring BIRT Analytics Loader
- Configuring BIRT Analytics connectors
- Configuring BIRT Analytics REST API
- Configuring BIRT Analytics FastDB

About the configuration files

This chapter describes the configuration files used by the applications in the BIRT Analytics system. The administrator edits these configuration files to adjust an application to the requirements of a production environment.

BIRT Analytics runs on Windows, LINUX or MAC systems, running as a service on Windows and as either a service or a process on LINUX or MAC.

The following BIRT Analytics applications run as web applications on an Apache Tomcat server.

- BIRT Analytics Application
- BIRT Analytics Administration
- BIRT Analytics Client
- BIRT Analytics Loader

All of these web applications (except BIRT Analytics Application) provide a user interface as webpages. Each application that has webpages uses an additional configuration file to set the appearance of those pages.

Additional files contain configuration settings for BIRT Analytics connectors, such as the BIRT Analytics REST API, and BIRT Analytics FastDB.

Configuring BIRT Analytics Application

BIRT Analytics Application is the web application that contains business logic and handles communication between the client application and the BIRT Analytics engine system.

BIRT Analytics Application reads configuration parameters from the file configuration.xml. On a Windows system, the location of configuration.xml is:

```
<BIRTAnalytics Installation folder>\ApplicationWS\WEB-INF\settings
```

On a Linux system, the location of configuration.xml is:

```
<BIRTAnalytics Installation folder>/ApplicationWS/WEB-INF/settings
```

Each parameter is an XML element in the <configuration> element. The value of the parameter is the element value.

Listing 2-1 shows the configuration settings in the configuration.xml file for BIRT Analytics Application installed in C:\BIRTAnalytics on a Windows system.

Listing 2-1 BIRT Analytics Application configuration settings

```
<configuration>
  <!-- license -->
  <license>C:\BIRTAnalytics\data\ApplicationWS\electron.lic</license>

  <!-- database settings -->
  <dbdriver>org.postgresql.Driver</dbdriver>
  <dburl>jdbc:postgresql://localhost:8111/wpt</dburl>
  <dbuser>user</dbuser>
  <dbpassword>password</dbpassword>
  <dbmaxactive>20</dbmaxactive>
  <dbmaxidle>10</dbmaxidle>
  <dbmaxwait>-1</dbmaxwait>

  <!-- uploading files. Unit is Kb -->
```

```

<maxmemsize>1024</maxmemsize>
<maxfilesize>51200</maxfilesize>

<!-- Actuate API WSDL file name -->
<actuateapiwsdl>ActuateAPI.wsdl</actuateapiwsdl>

<!-- directories -->
<mapdir>C:\BIRTAalytics\data\ApplicationWS\map</mapdir>
<stylesdir>C:\BIRTAalytics\data\ApplicationWS\styles</stylesdir>
<cachedir>C:\BIRTAalytics\data\ApplicationWS\cache</cachedir>
<importdir>C:\BIRTAalytics\data\ApplicationWS\import</importdir>
<exportdir>C:\BIRTAalytics\data\ApplicationWS\export</exportdir>
<campaigndir>C:\BIRTAalytics\data\ApplicationWS\campaign</campaigndir>

<!-- fastdb engine settings -->
<engineuser>SYSTEM</engineuser>
<enginepwd>PASSWORD</enginepwd>
<engineserver>localhost</engineserver>
<engineport>8105</engineport>
<engineignoredangerous>>false</engineignoredangerous>
<enginesecure>>false</enginesecure>
<enginemaxconnection>127</enginemaxconnection>
<enginemaxpoolEntries>127</enginemaxpoolEntries>

<!-- collect data for statistics -->
<columnstatistics>1</columnstatistics>

<!-- crosstab settings -->
<crosstabpagesize>1000</crosstabpagesize>
<!-- languages -->
<defaultlanguage>en_US</defaultlanguage>

<!-- association rule settings -->
<maxPageSizeReadingTransactionsForAssociationRuleAnalysis>10000</
  maxPageSizeReadingTransactionsForAssociationRuleAnalysis>
<maxTransactionsAllowedForAssociationRuleAnalysis>10000000</
  maxTransactionsAllowedForAssociationRuleAnalysis>
<maxItemsAllowedForAssociationRuleAnalysis>10000000</
  maxItemsAllowedForAssociationRuleAnalysis>
<maxRulesAllowedForAssociationRuleAnalysis>1000</
  maxRulesAllowedForAssociationRuleAnalysis>
<!-- time series forecasting settings -->
<maxPastIntervalsAllowed>1000</maxPastIntervalsAllowed>

<!-- sensitive log file -->
<sensitivelogfile>C:\BIRTAalytics\log\electronsensitive.log</
  sensitivelogfile>
<!-- location of BAConnectors -->
<baconnector>http://localhost:8110/baconnectors/metainf</baconnector>
<baconnectordata>http://localhost:8110/baconnectors/data</
  baconnectordata>
</configuration>

```

Configuring BIRT Analytics Administration

BIRT Analytics Administration is the web application that the administrator uses to configure the system.

BIRT Analytics Administration reads configuration parameters from the file configuration.xml. BIRT Analytics Administration reads user interface configuration

parameters from the file `clientsettings.xml`. On a Windows system, the location of the configuration files is:

```
<BIRTAnalytics Installation folder>\Administration\WEB-INF\settings
```

On a Linux system, the location of the configuration files is:

```
<BIRTAnalytics Installation folder>/Administration/WEB-INF/settings
```

Each configuration parameter in `configuration.xml` is an XML element in the `<configuration>` element. The value of the parameter is the element value.

Listing 2-2 shows the configuration settings in the `configuration.xml` file for BIRT Analytics Administration.

Listing 2-2 BIRT Analytics Administration configuration settings

```
<configuration>
  <urlclient>client/build/client.jsp</urlclient>
  <title>BIRT Analytics Administration</title>
  <ignoresslerrors>1</ignoresslerrors>
  <!-- uploading files. Unit is Kb -->
  <maxmemsize>1024</maxmemsize>
  <maxfilesize>51200</maxfilesize>
  <uploadsfolder>uploads</uploadsfolder>
  <!-- electron WS location and namespace -->
  <electronurl>http://localhost:8110/electronws/services</electronurl>
  <electronqname>http://services.ws.electron.ba.actuate.com</electronqname>
  <electronns>com.actuate.ba.electron.ws.services</electronns>
  <!-- session timeout params -->
  <msginterval>60000</msginterval>
  <sessiontimeout>180000</sessiontimeout>
  <!-- iHub settings -->
  <ihubidentityproviderurl>http://localhost:8000</ihubidentityproviderurl>
  <webappidentityid>http://localhost:8110/baadmin</webappidentityid>
</configuration>
```

Each user interface configuration parameter in `clientsettings.xml` is an XML `<setting>` element in the `<settings>` element. The name of the parameter is the value of the `name` attribute. The value of the parameter is the element value.

Listing 2-3 shows the user interface configuration settings in the `clientsettings.xml` file for BIRT Analytics Administration.

Listing 2-3 BIRT Analytics Administration user interface configuration settings

```
<settings>
  <setting name="resourceUri">resource</setting>
  <setting name="wsBase">/baadmin</setting>
  <setting name="wsBaseFrontend">/bafontend</setting>
  <setting name="wsBaseQloader">/qloader</setting>
  <setting name="wsBaseIPortal">:8700/iportal</setting>
  <setting name="dispatcher">/dispatcher</setting>
  <setting name="filetransfer">/filetransfer</setting>
  <setting name="upload">/upload</setting>
  <setting name="help">/help</setting>
  <setting name="sendByPost">/sendbypost.jsp</setting>
  <setting name="timeout">600000</setting>
  <setting name="dispatcherUri">../../../../dispatcher</setting>
  <setting name="debug">1</setting>
  <setting name="wrongResponseBehaviour">silent</setting>
  <setting name="msgInterval">60000</setting>
  <setting name="applicationName">BIRT Analytics</setting>
```

```

<setting name="discreteValuesPageSize">100</setting>
<setting name="decodePageSize">100</setting>
<setting name="dataExplorerPageSize">50</setting>
<setting name="discreteValuesExplorerPageSize">100</setting>
<setting name="debug">1</setting>
<setting name="crosstabMaxDV">100</setting>
<setting name="flashVersion">8.0.0</setting>
<setting name="evolution.discretValues">100</setting>
<setting name="map.discretValues">5000</setting>
<setting name="treeDiagramMaxItems">200</setting>
<setting name="fusionchartpage">fusionchartpage.jsp</setting>
<setting name="venndiagram">venn.jsp</setting>
<setting name="mappage">map.jsp</setting>
<setting name="svgviewer">svgviewer.jsp</setting>
<setting name="chartprinter">chartimage</setting>
<setting name="plugins">/client/frontend/application/plugins/build/
</setting>
<setting name="chartsRelativeUri">/graphics/</setting>
<!-- information about the application -->
<setting name="baversion">5.2.985</setting>
<setting name="qloaderappname">QLoader</setting>
</settings>

```

Configuring BIRT Analytics Client

BIRT Analytics Client is the web application that an end user uses to interact with the BIRT Analytics system.

BIRT Analytics Client reads configuration parameters from the file configuration.xml. BIRT Analytics Client reads user interface configuration parameters from the file clientsettings.xml. On a Windows system, the location of the configuration files is:

```
<BIRTAnalytics Installation folder>\WebClient\WEB-INF\settings
```

On a Linux system, the location of the configuration files is:

```
<BIRTAnalytics Installation folder>/WebClient/WEB-INF/settings
```

Each configuration parameter in configuration.xml is an XML element in the <configuration> element. The value of the parameter is the element value.

Listing 2-4 shows the configuration settings in the configuration.xml file for BIRT Analytics Client.

Listing 2-4 BIRT Analytics Client configuration settings

```

<configuration>
  <urlclient>client/build/client.jsp</urlclient>
  <title>BIRT Analytics</title>
  <ignoresslerrors>1</ignoresslerrors>
  <!-- uploading files. Unit is Kb -->
  <maxmemsize>1024</maxmemsize>
  <maxfilesize>50000000</maxfilesize>
  <!-- electron WS location and namespace -->
  <electronurl>http://localhost:8110/electronws/services</electronurl>
  <electronqname>http://services.ws.electron.ba.actuate.com</electronqname>
  <electronns>com.actuate.ba.electron.ws.services</electronns>
  <!-- session timeout params -->
  <msginterval>60000</msginterval>
  <sessiontimeout>180000</sessiontimeout>

```

```

<!-- Electron URL to transfer -->
<electronfiletransfer>/filetransfer</electronfiletransfer>
<electronupload>/uploader</electronupload>
<uploadsfolder>/uploads</uploadsfolder>
<!-- iHub settings -->
<ihubidentityproviderurl>http://localhost:8000</ihubidentityproviderurl>
<webappidentityid>http://localhost:8110/bafrontend</webappidentityid>
</configuration>

```

Each user interface configuration parameter in clientsettings.xml is an XML <setting> element within the <settings> element. The name of the parameter is the value of the name attribute. The value of the parameter is the element value.

Listing 2-5 shows the user interface configuration settings in the clientsettings.xml file for BIRT Analytics Client.

Listing 2-5 BIRT Analytics Client user interface configuration settings

```

<settings>
  <setting name="resourceUri">resource</setting>
  <setting name="wsBase">/bafrontend</setting>
  <setting name="wsBaseAdmin">/baadmin</setting>
  <setting name="wsBaseQloader">/qloader</setting>
  <setting name="wsBaseIportal">:8700/iportal</setting>
  <setting name="dispatcher">/dispatcher</setting>
  <setting name="filetransfer">/filetransfer</setting>
  <setting name="upload">/upload</setting>
  <setting name="help">/help</setting>
  <setting name="sendByPost">/sendbypost.jsp</setting>
  <setting name="timeout">6000000</setting>
  <setting name="dispatcherUri">../../../../dispatcher</setting>
  <setting name="debug">1</setting>
  <setting name="wrongResponseBehaviour">silent</setting>
  <setting name="msgInterval">60000</setting>
  <setting name="applicationName">BIRT Analytics</setting>
  <setting name="discreteValuesPageSize">100</setting>
  <setting name="decodePageSize">100</setting>
  <setting name="dataExplorerPageSize">50</setting>
  <setting name="discreteValuesExplorerPageSize">100</setting>
  <setting name="debug">1</setting>
  <setting name="crosstabMaxDV">100</setting>
  <setting name="evolution.discretValues">100</setting>
  <setting name="map.discretValues">5000</setting>
  <setting name="treeDiagramMaxItems">200</setting>
  <setting name="fusionchartpage">fusionchartpage.jsp</setting>
  <setting name="venndiagram">venn.jsp</setting>
  <setting name="mappage">map.jsp</setting>
  <setting name="svgviewer">svgviewer.jsp</setting>
  <setting name="chartprinter">chartimage</setting>
  <setting name="treeviewer">treediagram.jsp</setting>
  <!-- information about the application -->
  <setting name="baversion">5.2.985</setting>
  <setting name="qloaderappname">QLoader</setting>
  <!-- BIRT application name -->
  <setting name="birt">BIRT</setting>
  <setting name="homepageurl">http://birtanalytics.actuate.com/</setting>
  <setting name="homepageurltext">Visit BIRT Analytics website</setting>
  <setting name="documentationurl">
    http://birtanalytics.actuate.com/documentation</setting>

```



```

<setting name="documentationurltext">BIRT Analytics Documentation Page
  </setting>
<setting name="trainingvideosurl">
  http://birtanalytics.actuate.com/training-videos</setting>
<setting name="trainingvideosurltext">Webcasts and Training Videos
  </setting>
<setting name="blogurl">http://blogs.actuate.com/analytics/</setting>
<setting name="blogurltext">Actuate Analytics Blog</setting>
<setting name="psurl">
  http://birtanalytics.actuate.com/professional-services</setting>
<setting name="psurltext">Professional Services for BIRT Analytics
  </setting>
<setting name="recentanalysiscount">10</setting>
<setting name="loadingpage">loadingpage.html</setting>
</settings>

```

Configuring BIRT Analytics Loader

BIRT Analytics Loader is the web application that reads configuration parameters from the file configuration.xml.

BIRT Analytics Loader reads configuration parameters from the file configuration.xml. BIRT Analytics Loader reads user interface configuration parameters from the file clientsettings.xml. On a Windows system, the location of the configuration files is:

```
<BIRTAnalytics Installation folder>\FastDB\Loader\WEB-INF\settings
```

On a Linux system, the location of the configuration files is:

```
<BIRTAnalytics Installation folder>/WebClient/WEB-INF/settings
```

Each configuration parameter in configuration.xml is an XML element in the <configuration> element. The value of the parameter is the element value.

Listing 2-6 shows the configuration settings in the configuration.xml file for BIRT Analytics Loader.

Listing 2-6 BIRT Analytics Loader configuration settings

```

<configuration>
  <projectspath>C:\Actuate3\BIRTAnalytics\data\FastDB\loading-projects
    </projectspath>
  <descriptor>descriptor.txt</descriptor>
  <urlclient>fastdbloader/build/client.jsp</urlclient>
  <urladmin>admin/build/client.jsp</urladmin>
  <title>BIRT Analytics QLoader</title>
  <transformationslist>transformations.xml</transformationslist>
  <ignoresslerrors>1</ignoresslerrors>
  <!-- uploading files. Unit is Kb -->
  <maxmemsize>1024</maxmemsize>
  <!-- uploading files. Unit is Kb. -1 or 0 mean no limit -->
  <maxfilesize>-1</maxfilesize>
  <connectionstringsfile>connectionstrings.xml</connectionstringsfile>
  <!-- electron WS location and namespace -->
  <electronurl>http://localhost:8110/electronws/services</electronurl>
  <electronqname>http://services.ws.electron.ba.actuate.com</electronqname>
  <electronns>com.actuate.ba.electron.ws.services</electronns>
  <!-- information -->
  <baversion>5</baversion>
</configuration>

```

Each user interface configuration parameter in clientsettings.xml is an XML <setting> element in the <settings> element. The name of the parameter is the value of the name attribute. The value of the parameter is the element value.

Listing 2-7 shows the user interface configuration settings in the clientsettings.xml file for BIRT Analytics Loader.

Listing 2-7 BIRT Analytics Loader user interface configuration settings

```
<settings>
  <setting name="resourceUri">resource</setting>
  <setting name="wsBase">/qloader</setting>
  <setting name="wsBaseFrontend">/bafrontend</setting>
  <setting name="wsBaseAdmin">/baadmin</setting>
  <setting name="dispatcher">/dispatcher</setting>
  <setting name="help">/help</setting>
  <setting name="sendByPost">/SendByPost.jsp</setting>
  <setting name="timeout">6000000</setting>
  <setting name="dispatcherUri">../../../../dispatcher</setting>
  <setting name="debug">1</setting>
  <setting name="wrongResponseBehaviour">silent</setting>
  <setting name="msgInterval">60000</setting>
  <setting name="applicationName">BIRT Analytics Loader</setting>
  <setting name="discretevaluespagesize">100</setting>
  <setting name="thousandseparator">,</setting>
  <setting name="decimalseparator">.</setting>
</settings>
```

Configuring BIRT Analytics connectors

BIRT Analytics connectors read configuration parameters from the file configuration.xml. On a Windows system, the location of configuration.xml is:

```
<BIRTAnalytics Installation folder>\Connectors\WEB-INF\settings
```

On a Linux system, the location of configuration.xml is:

```
<BIRTAnalytics Installation folder>/Connectors/WEB-INF/settings
```

Each parameter is an XML element in the <configuration> element. The value of the parameter is the element value.

Configuring BIRT Analytics REST API

BIRT Analytics REST API reads configuration parameters from the file configuration.xml. On a Windows system, the location of configuration.xml is:

```
<BIRTAnalytics Installation folder>\restAPI\WEB-INF\settings
```

On a Linux system, the location of configuration.xml is:

```
<BIRTAnalytics Installation folder>/restAPI/WEB-INF/settings
```

Each parameter is an XML element in the <configuration> element. The value of the parameter is the element value.

Listing 2-8 shows the configuration settings in the configuration.xml file for BIRT Analytics REST API.

Listing 2-8 BIRT Analytics REST API configuration settings

```
<configuration>
  <electronurl>http://localhost:8110/electronws</electronurl>
  <bootstrap>http://localhost:8110/restapi/rest</bootstrap>
</configuration>
```

Configuring BIRT Analytics FastDB

BIRT Analytics FastDB engine, also known as the dubnium engine, is a web-based, Extract, Transform, and Load (ETL) service that reads most data sources. On a Windows system, the default location and name of the dubnium executable file is:

```
<BIRTAnalytics Installation folder>\FastDB\dubnium.exe
```

On a Linux system, the default location and name of the dubnium executable file is:

```
<BIRTAnalytics Installation folder>/FastDB/dubnium
```

FastDB runs by default when BIRT Analytics starts. On a Windows system, FastDB typically runs as a Windows service, named BIRT Analytics - FastDB. FastDB reads configuration parameters from the file `engine_configuration.ini`. On a Windows system, the location of `engine_configuration.ini` is:

```
<BIRTAnalytics Installation folder>\data\FastDB
```

On a Linux system, the location of `engine_configuration.ini` is:

```
<BIRTAnalytics Installation folder>/data/FastDB
```

The configuration file contains only parameters that require a non-default value. As shown in Listing 2-9, parameters are grouped by the functionality they affect. To set a value for a parameter, place the parameter name, an equal sign, and the value on a single line in the appropriate group. Listing 2-9 shows the `engine_configuration.ini` code for BIRT Analytics FastDB installed in C:\BIRTAnalytics on a Windows system.

Listing 2-9 `engine_configuration.ini` initial contents

```
[engine]
  license = C:\BIRTAnalytics\data\FastDB\dubnium.lic
  repository = C:\BIRTAnalytics\data\FastDB\databases
  exchange_path = C:\BIRTAnalytics\data\FastDB\exchange

[log]
  path = C:\BIRTAnalytics\log\engine.log
  verbosity = 6
  dbfibrillator_path = C:\BIRTAnalytics\log\dbfibrillator.log

[server]
  admin_file_path = C:\BIRTAnalytics\data\FastDB\admin.sqlite
  port = 8105
  threads = 2

[memory]
  maxmemorysystem = 4914
  maxmemorythread = 2457
```

Table 2-3 lists and describes the parameters that have a generic effect. These parameters have no default value. To set values for these parameters, place them at the beginning of the configuration file.

Table 2-3 BIRT Analytics FastDB overall parameters

Parameter	Description	Default value
batch	The name of a batch file to run	
password	The password for the user that runs the batch file	
user	The user that runs the batch file	
working	The folder to use as the context for the batch file	

Table 2-4 lists and describes the parameters that configure the FastDB engine. To set values for these parameters, place them in the [engine] section of the configuration file.

Table 2-4 BIRT Analytics FastDB engine configuration parameters

Parameter	Description	Default value
autocleanup	Whether to perform automatic clean-up of the FastDB repository cache. Set to 0 to disable automatic cache clean-up.	1
autolinkjumps	The number of jumps to accept before creating a new link automatically.	1
autoregeneratederived	Whether to perform automatic regeneration of derived columns. Set to 0 to disable automatic regeneration.	1
cxcachepagesize	The internal crosstab cache size. Do not change this value.	100000
cache_path	The path that contains the repository cache. The value is relative to the repository path.	cache
defaultpagesize	The default page size, which is the number of values returned in a request of discrete values of a column. This parameter takes effect only if the discreteValuesPageSize parameter in the BIRT Analytics web application clientsetting.xml file is changed accordingly.	100
defaultprecision	The default number of digits to display after the decimal point for numeric values.	2
exchange_path	The path to the folder containing import and export files.	<BIRTAnalytics Installation folder>\data\FastDB \exchange
firstdiscretethreshold	Number of rows after which to change strategy in first discrete operation.	1024
license	The path and name of the BIRT Analytics license file.	<BIRTAnalytics Installation folder>\data\FastDB \dubnium.lic

Table 2-4 BIRT Analytics FastDB engine configuration parameters

Parameter	Description	Default value
locale	The system wide locale. The locale determines the language used for error messages, date and time formats, and numeric symbols for thousands separator and decimal point. The locale format uses the standard Java convention of a two-letter language code, an underscore (_) character, and a two-letter country code. If translated messages are not available for the specified value, FastDB uses US English messages.	en_US
max_cache_size	The maximum size of the repository cache, in megabytes (MB). A value of 0 denotes no limit to the cache size.	0
max_dichotomous_columns	The maximum number of dichotomous columns to create from discrete values.	16
maximumprecision	The maximum number of digits to display after the decimal point for numeric values.	8
max_pivot_values	The maximum number of discrete values in a crosstab column to use as a pivot column.	1024
nonlinked_aggregated	Whether to aggregate crosstabs non-linked record values in a row. Set to 1 to aggregate values.	0
repository	The engine repository path.	<BIRTAnalytics Installation folder>\data\FastDB \databases

Table 2-5 lists and describes the parameters that configure the FastDB logs. To set values for these parameters, place them in the [log] section of the configuration file.

Table 2-5 BIRT Analytics FastDB log configuration parameters

Parameter	Description	Default value
communication	Whether to log the request and response communications with the server. Set to 1 to enable communication logging.	0
dbfibrillator_path	The path and name of the dbfibrillator server log file. The dbfibrillator server monitors the FastDB engine restarts the engine after a failure.	<BIRTAnalytics Installation folder>\log \dbfibrillator.log
expressions	Whether to log the syntax trees of expressions. Set to 1 to enable expression logging.	0
path	The path and name of the log file.	<BIRTAnalytics Installation folder>\log \engine.log
verbosity	An integer value denoting the level of detail to log. A smaller value logs less information. Valid values are 6 for INFORMATIONAL level and 7 for DEBUG level.	6

Table 2-6 lists and describes the parameters that configure the FastDB memory usage. To set values for these parameters, place them in the [memory] section of the configuration file.

Table 2-6 BIRT Analytics FastDB memory configuration parameters

Parameter	Description	Default value
buffer_size_datasources	Datasources buffer size in kilobytes (KB).	8192
maxmemorysystem	Maximum system memory in megabytes (MB). Estimate the maximum value using the following formula: [Server memory] - ([OS memory] * 2	4096
		<i>(continues)</i>
maxmemorythread	Maximum thread memory in megabytes. Each engine request uses a separate thread. Total memory usage for threads cannot exceed maxmemorysystem. Set the value for maxmemorythread according to the number of predicted concurrent requests.	2048
memorylogenabled	Whether to enable memory logging. This parameter takes effect only when log verbosity is at DEBUG level. Set to 0 to disable memory logging even at DEBUG log verbosity.	1

Table 2-7 lists and describes the parameters that configure the FastDB remote data provider. To set values for these parameters, place them in the [rdp] section of the configuration file.

Table 2-7 BIRT Analytics FastDB remote data provider (RDP) configuration parameters

Parameter	Description	Default value
ca_cert	A public transport layer security (TLS) certificate authority (CA) file.	
connect_timeout	The connection time-out to the RDP server in seconds.	30
password	The password for the account specified by the username parameter.	
proxy_addr	The IP address of the proxy server.	
proxy_exceptions	A comma-separated list of hosts that do not use a proxy.	
proxy_password	The password for the account specified by the proxy_username parameter.	
proxy_port	The port on which to access the proxy server.	8080
proxy_type	The proxy type. One of the following values: <ul style="list-style-type: none"> ■ HTTP ■ HTTP_1_0 ■ SOCKS4 ■ SOCKS5 ■ SOCKS4A ■ SOCKS5_HOSTNAME 	HTTP
proxy_username	The name of the account used to access the proxy server.	

Table 2-7 BIRT Analytics FastDB remote data provider (RDP) configuration parameters

Parameter	Description	Default value
ssl_verify	Whether to verify the transport layer security (TLS) certificate against a certificate authority (CA). Set to 1 to use a CA.	0
timeout	Execution time-out in seconds.	60
use_proxy	Whether to use a proxy server to connect to the RDP source. Set to 1 to use a proxy.	0
username	The account name for RDP server authentication.	

Table 2-8 lists and describes the parameters that configure the FastDB server. To set values for these parameters, place them in the [server] section of the configuration file.

Table 2-8 BIRT Analytics FastDB server configuration parameters

Parameter	Description	Default value
admin_file_path	Authentication and security file path. The default location for the file is: <BIRTAnalytics Installation folder> \data\FastDB	admin.sqlite
cert_country	Server certificate data: the country as a Java standard two-character code.	US
cert_email	Server certificate data: the contact e-mail address. For example, administrator@yourdomain.com.	
certificate	Server public certificate. The default location for the file is: <BIRTAnalytics Installation folder> \data\FastDB	server.pem
cert_locality	Server certificate data: the locality, which is a city or town. For example, New York or Barcelona.	
cert_organization	Server certificate data: organization or company name. For example, OpenText.	
cert_service_names	Server certificate separated service names. For example, yourcompany.com,192.168.0.55.	
cert_state	Server certificate data: the state. For example, Texas.	
connectiontimeout	Time-out of the connection to the engine, in milliseconds. FastDB closes the connection if no activity occurs in this period of time. A value of 0 denotes that the connection never times out.	0
daemon_pidfile	For internal use. Do not change this value.	dubnium.pid
dh_filename	Diffie-Hellman parameters file. The default location for the file is: <BIRTAnalytics Installation folder> \data\FastDB	dhparams.pem
enable_daemon	For internal use. Do not change this value.	0

(continues)

Table 2-8 BIRT Analytics FastDB server configuration parameters (continued)

Parameter	Description	Default value
enable_dbfibrillator	Whether to enable automatic restart in case of failure or a crash. Set to 0 to disable automatic restart.	1
enable_insecure_port	Start a listener on the non-secure, standard port, specified by the port parameter on the system specified by the ip parameter. Set to 0 to disable this port.	1
enable_secure_port	Start a listener on the secure, TLS port, specified by the secure_port parameter on the system specified by the ip parameter. Set to 1 to enable this port.	0
ip	Listener IP address. This system uses the ports specified by the port and secure_port parameters.	0.0.0.0
maxrequestlen	Maximum length of the request XML accepted by the FastDB engine. A request is a selection or domain specified by the user.	65535
port	Listener port for non-secure connections on the system specified by the ip parameter.	8105
private_key	Server private key. The default location for the file is: <BIRTAnalytics Installation folder> \data\FastDB	server.key
private_key_password	Password for server private key.	
rand_filename	Random number file used for TLS calculations. The default location for the file is: <BIRTAnalytics Installation folder> \data\FastDB	ssl.rnd
root_ca_certificate	Root certificate authority (CA) public certificate. The default location for the file is: <BIRTAnalytics Installation folder> \data\FastDB	cacert.pem.
secure_port	Listener port for secure connections on the system specified by the ip parameter.	8106
ssl_mode	Certificate mode for transport layer security (TLS). The following values are valid: <ul style="list-style-type: none"> ■ simple to use a self-signed certificate ■ complete to use a root certificate authority (CA) 	simple
threads	Maximum threads per FastDB server.	5
winsvc_pass	Windows service registration password. Set a value to use a specific user rather than the default Local System account.	
winsvc_user	Windows service registration user name. Set a value to use a specific user rather than the default Local System account.	

Part Two

Administering BIRT Analytics reference

- Administering BIRT Analytics functional reference

3

Administering BIRT Analytics functional reference

This chapter is a reference section describing the functionalities that the administrator uses to configure permissions in the security role management module of BIRT Analytics Administration.

Administering BIRT Analytics functional reference

This chapter is a reference section describing the functionalities that the administrator uses to configure permissions in the security role management module of BIRT Analytics Administration. Each category section provides the name of the parameter along with a description of its function in the BIRT Analytics system.

The parameters in the tables are listed typically in the order of occurrence. The tables at the beginning of each section describe functionalities that have no subordinate items in the lists. Complex sets of functionalities that contain subordinate items are grouped into tables by category. In some cases, these tables group closely related categories together, rather than by order of occurrence, to make referencing related items more convenient.

In the Security role management module Functionalities list, select + to expand a functional category. Select the higher-level category to include all the subordinate elements or select elements individually in the category lists to configure a more restricted subset of privileges.

General

Table 3-1 describes the functionalities that have no subordinate items in the General list.

Table 3-1 General functionalities

Functionality	Description	Module
Change resolution level	Controls ability to change resolution level in a domain.	Admin
Check active LDAP	Controls access to information about type of active security.	Admin
Convert ID to name	Obsolete.	
Convert name to ID	Obsolete.	
Count discrete values	Provides access to the number of discrete values in a column to determine the value of a specific action.	Frontend: Analysis (manipulation of segments)
Data tree	Obtains structure of the database.	Frontend: Data Tree, Bloc of notes (change resolution)
Discrete values of a domain	Allows user to generate domains of discrete values from another domain.	Bloc of notes (discrete values)
Get header image	Allows uploading server header image for export to RTF.	Jetadmin: Management Style
Get higher tables	Allows user to access higher tables.	Frontend: Multiple sites
Get LDAP groups	Controls access to information about active security groups.	Admin
Get resolution level	Controls access to resolution level in a domain.	Frontend: Explorer (data, export, analysis Venn, internal use of segments)

Table 3-1 General functionalities (continued)

Functionality	Description	Module
Get RTF styles	Gets RTF style definition.	Frontend: Export RTF
Get user functionalities	Controls access to user functionality information.	Admin
Get user information	Controls access to basic user information.	Admin
Insert a new configuration setting	Allows user to insert a new configuration key.	Admin
Load data from a folder	Allows data analysis using the shared folder of another user.	Frontend: Folder Tree
Operate with domains	Allows operations between domains.	Frontend: Bloc of notes, Analysis, explore data
Prepare saved cross tab for execution	Allows preparation of a crosstab analysis for execution.	Analysis: Crosstab
Put RTF styles	Sets style for RTF export.	Frontend: Export RTF
Read configuration setting	Allows user to read a configuration key.	Admin
Selections— Calculate selection	Controls access to module selection. Allows user to execute selection.	Frontend: Selections
Sort Domains	Allows user to arrange domains in Bloc of notes.	Frontend: Bloc of notes
Upload header image	Allows uploading header image to server for export to RTF.	Frontend: Export RTF
Validate discrete column	Checks if a column is completely discrete.	Plugin: iWorkflow
Validate LDAP settings	Allows validating type of active security.	Admin
Validate Login	Allows system to manage anonymous user access.	Admin
View columns— Change Indexing	Allows user to index a column in the repository.	Frontend: Data Tree
View columns— Index column	Allows user to index an unindexed column	Frontend: Data Tree
View columns— Unindex column	Allows user to unindex an indexed column	Frontend: Data Tree
View databases	Allows user to access list of available databases.	Frontend: Data Tree

(continues)

Table 3-1 General functionalities (continued)

Functionality	Description	Module
View discrete values	Limits access to discrete values of a column.	Frontend: Data Tree, Explorer (discrete and graphic values field), Evolution Analysis, Engineering (Decoder)
View object data	Allows access to database object information.	Frontend
View parent table	Allows viewing parent table for a specific table in the database.	Frontend: Multiple modules
View tables	Allows viewing tables from a specific database.	Frontend: Data Tree
View user functionalities	Controls access to user functionality information.	Admin

Administration

This section describes the Administration functionalities used in configuring the BIRT Analytics environment.

Administration

Table 3-2 describes the functionalities that have no subordinate items in the Administration list.

Table 3-2 Administration functionalities

Functionality	Description	Module
Administration	Controls settings for all Administration management functionalities	Admin
Add password policy	Controls ability to define rules for user passwords	Admin
Create key fields	Allows administrator to create new key fields	Admin
Delete sensitive column	Limits ability to unmark a column from the repository as a sensitive column	Admin
Insert sensitive column	Limits ability to mark a column from the repository as a sensitive column	Admin
Get sensitive columns	Controls access to the list of sensitive columns	Admin
Get ACL	Controls access to information on relationships between an object, groups, and users	Admin
Get active engine settings	Controls access to current engine configuration settings	Admin
Get functionalities map	Controls access to information on relationships between functionalities, roles, and users	Admin

Table 3-2 Administration functionalities

Functionality	Description	Module
Get Pool Connections status	Controls access to information about connection pool	Admin
List security policies	Controls access to the rules required in adding a user password	Admin
Update security policies	Controls ability to modify rules for user passwords	Admin
Purge obsolete connections	Controls ability to delete current connections to analytical engine	Admin
Read application log	Controls access to the log that creates a record of activity on the system	Admin

Access control list (ACL)

Table 3-3 describes the security group and filter functionalities that control access control list (ACL) management.

Table 3-3 Access control list (ACL) functionalities

Functionality	Description	Module
ACL	Controls settings for all security group and filters management functionalities	Admin: Security
Delete security filter	Controls the elimination of security filter	Admin: Security
Delete security group	Controls the elimination of security group	Admin: Security
Edit security filter	Controls the modification of an existing security filter	Admin: Security
Edit security group	Controls the modification of security group	Admin: Security
Get mapped database structure	Controls access to repository database mappings	Frontend: Data Tree
Get object authorizations	Controls access to object authorizations	Admin: Security
Get security filter	Controls access to security filter	Admin: Security
Get security filters	Controls access to multiple security filters	Admin: Security
Get security group	Controls access to security group	Admin: Security
Get security groups	Controls access to multiple security groups	Admin: Security
		<i>(continues)</i>
Give access to security group	Grants access by a security group to specified data objects	Admin: Security
New security filter	Controls the creation of a new security filter	Admin: Security

Table 3-3 Access control list (ACL) functionalities (continued)

Functionality	Description	Module
New security group	Controls the creation of security group	Admin: Security
Remove authorizations to security group	Revokes access by a security group to specified data objects	Admin: Security

Configuration

Table 3-4 describes the Configuration functionalities that control Simple Mail Transfer Protocol (SMTP) management.

Table 3-4 Configuration functionalities

Functionality	Description	Module
Configuration	Controls settings for all Configuration functionalities.	Admin: Configuration
Get SMTP configuration	Controls access to SMTP settings. Specifies Get SMTP configuration property only.	Admin: Configuration
Set SMTP configuration	Controls permission to change SMTP settings. Specifies Set SMTP configuration property only.	Admin: Configuration

Folders

Table 3-5 describes the functionalities that control folder management.

Table 3-5 Folders functionalities

Functionality	Description	Module
Folders	Controls settings for all Folders functionalities	Frontend: Data Tree
Create folder	Allows a user to create a file or folder for storing analysis selections	Frontend: Data Tree, Analysis (process to save analysis)
Delete folder	Allows a user to delete a file or folder	Frontend: Data Tree
Edit folder	Allows a user to edit a file or folder	Frontend: Data Tree
View folders	Allows a user to access the related list of files and analysis items	Frontend: Data Tree
View folders and items	Allows a user to access the related list of files and analysis items	Frontend: Data Tree

Functionalities

Table 3-6 describes the settings that control functionalities management.

Table 3-6 Functionalities settings

Functionality	Description	Module
Functionalities	Controls ability to manage the Functionalities list	Admin

Table 3-6 Functionalities settings

Functionality	Description	Module
View functionality tree	Controls access to the functionalities list	Admin

Groups

Table 3-7 describes the functionalities that control group management.

Table 3-7 Groups functionalities

Functionality	Description	Module
Groups	Controls settings for all Groups functionalities	Admin: Groups Management
Create group	Allows creating a group	Admin: Groups Management
Delete group	Allows deleting a group	Admin: Groups Management
Edit group	Allows editing a group	Admin: Groups Management
View group	Allows viewing information for a group	Admin: Groups Management
View groups	Allows viewing a list of groups	Admin: Groups Management

Integrity

Table 3-8 describes the functionalities that control integrity management.

Table 3-8 Integrity functionalities

Functionality	Description	Module
Integrity	Controls settings for all Integrity functionalities. Configures synchronization between Administration application and data repository.	Admin
Delete temporary items	Controls elimination of cache files from the server.	Admin
Get temporary information	Allows administrator to obtain information regarding repository column use.	Admin
Purge erroneous ACL entries	Allows purging obsolete permits applied to nonexistent objects.	Admin
Synchronize structure to repository	Allows synchronization of data structure with repository.	Admin

(continues)

Profile

Table 3-9 describes the functionalities that control profile management.

Table 3-9 Profile functionalities

Functionality	Description	Module
Create Profile	Allows creating a profile	Admin
Delete Profile	Allows deleting a profile	Admin
Edit Profile	Allows editing a profile	Admin
Load Profile	Controls access to property information for a specific profile	Admin
Get profiles list	Controls access to a profile list	Admin

Roles

Table 3-10 describes the functionalities that control role management.

Table 3-10 Roles functionalities

Functionality	Description	Module
Roles	Controls settings for all Roles functionalities	Admin: Security Role Management
Create role	Allows creating a role	Admin: Security Role Management
Delete role	Allows deleting a role	Admin: Security Role Management
Edit role	Allows deleting a role	Admin: Security Role Management
View role	Allows viewing information for a role	Admin: Security Role Management
View roles	Allows viewing a list of roles	Admin: Security Role Management

Users

Table 3-11 describes the functionalities that control user management.

Table 3-11 Users functionalities

Functionality	Description	Module
Users	Controls settings for all Users functionalities.	Admin: User Management
Create user	Allows creating a user.	Admin: User Management
Delete user	Allows deleting a user.	Admin: User Management

Table 3-11 Users functionalities

Functionality	Description	Module
Edit user	Allows editing a user. An update done in the frontend is limited to the number of modifiable attributes for the user.	Admin: User Management; Frontend: User Preference
View user	Allows viewing information for a user.	Admin: User Management
View users	Allows viewing a list of users.	Admin: User Management

Analysis

This section describes the Analysis functionalities used in configuring the BIRT Analytics environment.

Analysis

Table 3-12 describes the functionalities that have no subordinate items in the Analysis list.

Table 3-12 Analysis functionalities

Functionality	Description	Module
Analysis	Controls settings for all Analysis functionalities.	Frontend: Data Tree
Change analysis	Allows user to modify an analysis definition.	Frontend: Data Tree
Clear recent analysis list	Allow user to clear Recenet Analysis list with saved analyses opened recently	Start: Recent Analysis
Delete analysis	Allows user to delete an analysis.	Frontend: Data Tree
Export saved analyses	Allows user to export saved analysis.	Frontend: Data Tree
Get list of authorizations for report	Allows user access to authorizations list for a report.	Frontend: Analysis/selections (save element)
Get recent analysis	Allows user access to Recent Analysis list.	Start: Recent Analysis
		<i>(continues)</i>
Get selection definition	Allows user access to selection definition.	Frontend: Analysis/selections (save element)
Get users to share analysis	Allows user access to list of users belonging to the same group who can share an analysis.	Frontend: Analysis/selections (save element)
Import analyses/selections	Allows user to import previously exported analysis.	Frontend: Data Tree
Open analysis	Allows user to open an analysis.	Frontend: Analysis/ selections.

Table 3-12 Analysis functionalities (continued)

Functionality	Description	Module
Save analysis	Allows user to save an analysis. Requires create folder privilege.	Frontend: Analysis/selections.

Bubble diagram

Table 3-13 describes the functionalities that control bubble diagram management.

Table 3-13 Bubble diagram functionalities

Functionality	Description	Module
Bubble diagram	Controls settings for all Bubble diagram functionalities	Analysis: Bubble
Calculate bubble diagram	Specifies Calculate bubble diagram property only	Analysis: Bubble
Run bubble diagram	Configures running all Run bubble diagram properties	Analysis: Bubble

Calculate Pareto

Table 3-14 describes the functionalities that control Pareto management.

Table 3-14 Pareto functionalities

Functionality	Description	Module
Calculate Pareto	Controls settings for all Calculate Pareto functionalities	Analysis: Pareto
Export Pareto	Specifies Export Pareto functionality	Analysis: Pareto

Crosstab

Table 3-15 describes the functionalities that control crosstab management.

Table 3-15 Crosstab functionalities

Functionality	Description	Module
Crosstab	Controls setting for all Crosstab functionalities	Analysis: Crosstab
Run Crosstab	Controls execution of a crosstab	Analysis: Crosstab
Export Crosstab	Allows user to export a crosstab analysis to an Ofimatic format	Analysis: Crosstab
Extract from Crosstab	Allows user to extract a domain from a crosstab analysis	Analysis: Crosstab

Evolution diagram

Table 3-16 describes the functionalities that control evolution diagram management.

Table 3-16 Evolution diagram functionalities

Functionality	Description	Module
Evolution diagram	Controls settings for all Evolution diagram functionalities	Frontend: Analysis (Evolution)

Table 3-16 Evolution diagram functionalities

Functionality	Description	Module
Export Evolution	Limits export of evolution analysis type	Frontend: Analysis (Evolution)

Gallery

Table 3-17 describes the functionalities that control gallery management.

Table 3-17 Gallery functionalities

Functionality	Description	Module
Gallery	Controls settings for all Gallery functionalities	Gallery
Calculate Gallery	Allows user to calculate a gallery measure definition	Gallery
Export Gallery	Allows user to export a gallery measure definition	Gallery
Get map to print Gallery	Allows user to get a map to print a gallery measure definition	Gallery

Map diagram

Table 3-18 describes the functionalities that control map diagram management.

Table 3-18 Map diagram functionalities

Functionality	Description	Module
Map diagram	Controls settings for all Map diagram functionalities.	Frontend: Analysis (Maps)
Calculate Map	Allows user to perform a Calculate Map operation	Frontend: Analysis (Maps)
Delete Map	Allows user to delete a map	Admin
Get Maps list	Allows user to get a map list	Frontend: Analysis (Maps)
Print Map	Allows user to print a map operation	Frontend: Analysis (Maps)
Upload Map	Allows user to upload a map	Admin
View Map	Allows user to view a map	Admin

Profile

Table 3-19 describes the functionalities that control profile management.

Table 3-19 Profile functionalities

Functionality	Description	Module
Profile	Controls settings for all Profile functionalities	Frontend: selection
Run Profile	Run Profile controls execution of the profile analysis type	Frontend: Analysis (Profile)

Table 3-19 Profile functionalities

Functionality	Description	Module
Export Profile	Export Profile enables a user to export the results of a profile analysis type	Frontend: Analysis (Profile)

Venn diagram

Table 3-20 describes the functionalities that control Venn diagram management.

Table 3-20 Venn diagram functionalities

Functionality	Description	Module
Venn diagram	Controls settings for all Venn diagram functionalities.	Analysis: Venn
Run Venn diagram	Controls execution of Venn diagram. Configures running export and extract Venn diagram properties.	Analysis: Venn
Export Venn diagram	Allows user to export a Venn analysis to an Ofimatic format.	Analysis: Venn
Extract from Venn diagram	Allows user to extract a domain from a Venn analysis.	Analysis: Venn

Data exploration

Table 3-21 describes the functionalities that control data exploration management.

Table 3-21 Data exploration functionalities

Functionality	Description	Module
Data Exploration	Controls settings for all Data Exploration functionalities.	Frontend: Explorer
Export statistics	Allows user to export statistics in RTF format.	Frontend: Explorer (statistics field)
Export summary	Allows user to export a summary for a table or field in file format.	Frontend: Explorer (summary field)
View discrete values graphic	Limits access to a discrete values graphic from a specific column.	Frontend: Explorer (discrete values graphic field)
View frequency distribution	Controls access to Frequency tab	Frontend: Explorer (frequency tab)
View records	Controls access to records in the database.	Frontend: Explorer
View statistics	Controls access to statistics for a field in the database.	Frontend: Explorer (register field)
View summary	Limits access to field and table summaries. User must have access to underlying data to view summary.	Frontend: Explorer (summary field)

Engine security

Table 3-22 describes the Engine security functionalities previously available in configuring the BIRT Analytics environment. These features are obsolete.

Table 3-22 Engine security functionalities

Functionality	Description	Module
Engine security	Obsolete	
View engine security filters	Obsolete	
View engine security groups	Obsolete	

Engineering

This section describes the Engineering functionalities used in configuring the BIRT Analytics environment.

Engineering

Table 3-23 describes the functionalities that have no subordinate items in the Engineering list.

Table 3-23 Engineering functionalities

Functionality	Description	Module
Engineering	Controls settings for all Engineering functionalities.	Frontend: Engineering
Clear table	Controls clearing a user table.	Frontend: Engineering
Create aggregate	Allows user create a new aggregated column.	Frontend: Engineering (create aggregated)
Create decoder	Allows user to create a new decode column.	Frontend: Engineering (create decode)
Create expression— Get engine functions	Create expression enables a user to create a new expression column. Get engine functions enables access to the list of functionalities available when creating a new field of expression type.	Frontend: Engineering (create expression)
Create numeric range— Get limits	Allows accessing the values needed to compose a new field of numeric rank type.	Frontend: Engineering (create numeric rank)
Create Parametric	Allows user to create a new parametric column.	Frontend: Engineering (create parametric)
Create quantile	Allows user to create a new column quantile type.	Frontend: Engineering (create quantile)

Table 3-23 Engineering functionalities

Functionality	Description	Module
Create Ranking	Allows user to create a new column with numeric ranking.	Frontend: Engineering (create numeric rank)
Delete column	Limits elimination of a column from the repository data.	Frontend: Data Tree
Drop database	Limits elimination of a database from the repository data.	Frontend: Data Tree
Make a column permanent	Allows user to make a column permanent when creating a new column.	Frontend: Navigation Tree
Make domain permanent	Allows user to make a domain permanent when creating a new domain.	Frontend: Bloc of notes (make permanent)
Rename object	Allows user to rename an object from the repository data (database, table, column).	Frontend: Data Tree
Validate expression	Allows user to validate an expression when creating an expression type field.	Frontend: Engineering (expression field)

Edit engineering fields

Table 3-24 describes the Update a column functionalities that control Edit engineering fields management.

Table 3-24 Edit engineering fields functionalities

Functionality	Description	Module
Edit engineering fields—Update a column	Controls settings for all Edit engineering fields functionalities. —Update a column functionalities list.	Frontend: Engineering
Clear dependent cache	Allows system to clear obsolete cache files due to changes in the repository.	Frontend: Internal
Get aggregate definition	Controls access to a aggregate-type field definition.	Frontend: Engineering (aggregated)
Get decoded definition	Controls access to a decoding-type field definition.	Frontend: Engineering (decode)
Get definition of an expression	Controls access to an expression type field definition.	Frontend: Engineering (expression)
Get numeric range definition	Controls access to a numeric-range-type field definition.	Frontend: Engineering (numeric range)
Get parametric definition	Controls access to a parametric-type field definition.	Frontend: Engineering (parametric)
Get quantile definition	Controls access to a quantile-type field definition.	Frontend: Engineering (quantile)

Table 3-24 Edit engineering fields functionalities (continued)

Functionality	Description	Module
Get ranking definition	Controls access to a ranking type field definition.	Frontend: Enrichment (ranking)
Get the definition from a domain field	Controls access to a domain type field definition	Frontend: Data tree
Update a column	Controls settings for all Update a column functionalities	Frontend: Engineering
Update aggregate	Controls modification of an aggregate-type field definition.	Frontend: Engineering (aggregated)
Update decoded	Controls modification of a decoding-type field definition.	Frontend: Engineering (decode)
Update expression	Controls ability to modify an expression type field definition.	Frontend: Engineering (expression)
Update numeric range	Controls modification of a numeric-range-type field definition.	Frontend: Engineering (numeric range)
Update parametric	Controls modification of a parametric-type field definition.	Frontend: Engineering (parametric)
Update quantile	Controls modification of a quantile-type field definition.	Frontend: Engineering (quantile)
Update ranking	Controls ability to modify a ranking type field definition.	Frontend: Enrichment (ranking)

Events and Alerts

Table 3-25 describes the functionalities that have no subordinate items in the Events and Alerts list.

Table 3-25 Events and Alerts functionalities

Functionality	Description	Module
Events and Alerts	Controls settings for all Events and Alerts functionalities	Admin/ Frontend
Create scheduled task	Allows user to create a scheduled task	Admin/ Frontend
Delete scheduled task	Allows user to delete a scheduled task	Admin/ Frontend
Events service management	Allows user to manage events service	Admin/ Frontend
Execute scheduled task	Allows user to execute a scheduled task	Admin/ Frontend

Table 3-25 Events and Alerts functionalities (continued)

Functionality	Description	Module
Get available actions by event	Allows user to get available actions by event	Admin/ Frontend
Get event detail	Allows user to get an event detail	Admin/ Frontend
Get events list	Allows user to get an event list	Admin/ Frontend
Get scheduled task	Allows user to get a scheduled task	Admin/ Frontend
Get scheduled task log	Allows user to get a scheduled task log	Admin/ Frontend
Get values list by attribute	Allows user to get a values list by attribute	Admin/ Frontend
Retrieve scheduled task	Allows user to retrieve a scheduled task	Admin/ Frontend

Actions

Table 3-26 describes the functionalities that control action management.

Table 3-26 Actions functionalities

Functionality	Description	Module
Actions	Controls settings for all Actions functionalities	Admin/ Frontend
Action drop database	Allows user access to Action eliminate a database from the repository data	Frontend Event and alerts - Actions
Action rename object	Allows user access to Action rename a repository object	Frontend Event and alerts - Actions
Apply Model Action	Allows user access to Action apply a model from a saved Data Mining analysis	Frontend Event and alerts - Actions
Delete column	Allows user to delete a column	Admin/ Frontend
Delete table	Allows user to delete a table	Admin/ Frontend
Evaluate condition	Allows user to evaluate a condition	Admin/ Frontend
Notify definition updates	Allows user to specify notification for a definition update	Admin/ Frontend
Send e-mail	Allows user to specify a send e-mail notification	Admin/ Frontend

Import-Export

Table 3-27 describes the functionalities that control import-export management.

Table 3-27 Import-Export functionalities

Functionality	Description	Module
Import-Export	Controls settings for all Import-Export functionalities	Frontend: Import
Abort execution	Allows user to cancel a loading process execution	Frontend: Load
Check datasource	Allows user to Test a data source definition	Frontend: Load
Clear imported file	Allows user to delete a file previously uploaded to the server	Frontend: Import
Create custom query	Allows user to Create a custom query in a data source	Frontend: Load
Create datasource	Allows user to Create a data source definition	Frontend: Load
Delete custom query	Allows user to Eliminate a custom query from a data source	Frontend: Load
Delete datasource	Allows user to Eliminate a data source definition	Frontend: Load
Delete execution	Allows user to Eliminate a history execution	Frontend: Load History
Export a domain to a scheduled task	Allows user to select data for export to a scheduled task	Frontend: Export
Export domain	Allows user to select data for export to files	Frontend: Export
Export analytical database domain	Allows user to select data for export to repository	Frontend: Export
<i>(continues)</i>		
Export bubble	Allows user to export a bubble analysis to an Ofimatic format	Frontend: Analysis Bubble
Export Holtwinters to PDF	Allows user to export a Forecasting analysis to an Ofimatic format	Frontend: Advanced Analysis
Export SVG to PDF	Allows user to export a map analysis to an Ofimatic format	Frontend: Analysis Map
Get columns from datasource	Allows user access to edit data source definition	Frontend: Load
Get datasources	Allows user access to select a data source type	Frontend: Load
Get deferred file as xml	Gets a deferred file in XML format	Engine and events alerts
Get definition from datasource	Get definition from data source	Frontend: Import

Table 3-27 Import-Export functionalities (continued)

Functionality	Description	Module
Get download shelf items list	Allows user to access an item list from the download shelf	Frontend: Downloads
Get download shelf types list	Allows user to access a types list from the download shelf	Frontend: Downloads
Get exported file	Allows a user access to an exported file	Frontend: Export
Get list of executions	Allows user access to history execution list	Frontend: Load History
Get ODBC information	Allows user access to edit an ODBC data source definition	Frontend: Load
Get sample from datasource	Allows user access to see a sample of data in File Properties editing a data source	Frontend: Load
Get tables from datasource	Allows user access to Tables of a data source definition	Frontend: Load
Get valid columns	Controls access to the list of columns available for export	Frontend: Export
Guess file format	Allows user to guess the file format of a text file when creating a data source definition	Frontend: Load
Import	Allows user to import analytical data from an external file previously uploaded to the server	Frontend: Import
Load custom query	Allows user to edit a custom query in a data source	Frontend: Load
Load datasource query	Allows user access to edit a data source definition	Frontend: Load
<i>(continues)</i>		
Load execution query	Allows user access to edit a loading process from History executed list	Frontend: Load History
Modify custom query	Allows user to modify a custom query in a data source	Frontend: Load
Modify datasource query	Allows user to midify a data source definition	Frontend: Load
Remove item from download shelf	Allows user to remove an item from the download shelf	Frontend: Downloads
Retrieve current execution	Retrieve current execution	Frontend: Import
Run loading project	Controls access to Execute a loading project	Frontend: Load
Streaming data export	Controls access to Streaming a data export	Frontend: Enrichment Export
Upload file	Allows user to upload a file to server for downloading at a later time	Frontend: Import

Links

Table 3-28 describes the functionalities that control link management.

Table 3-28 Links functionalities

Functionality	Description	Module
Links	Control settings for all Links functionalities	Frontend: Links
Create link	Allows user to create a new link to an object in a database	Frontend: Links
Delete broken links	Allows user to delete a broken link	Frontend: Links
Delete link	Allows user to delete a link	Frontend: Links
Delete temporary links	Allows user to delete a temporary link	Frontend: Links
View links	Allows user to view a link	Frontend: Links

Plug-ins

This section describes the Plug-ins functionalities used in configuring the BIRT Analytics environment.

Plug-ins

Table 3-29 describes the functionalities that control plug-in management.

Table 3-29 Plug-ins functionalities

Functionality	Description	Module
Plug-ins	Controls settings for all Plug-ins functionalities	Frontend: Internal

Cworkflow

Table 3-30 describes the functionalities that control Cworkflow management.

Table 3-30 Cworkflow functionalities

Functionality	Description	Module
Cworkflow	Controls settings for all workflow management options	Plugin: Cworkflow
Display "Levels Management" option	Displays Levels Management option	Plugin: Cworkflow
Show "Actions Management" option	Displays Actions Management option	Plugin: Cworkflow

Table 3-30 Cworkflow functionalities (continued)

Functionality	Description	Module
Show "Campaign Management" option	Displays Campaign Management option	Plugin: Cworkflow
Show "Campaign Planning" option	Displays Campaign Planning option	Plugin: Cworkflow
Show "Media Management" option	Displays Media Management option	Plugin: Cworkflow
Show "Workflow Management" option	Displays Workflow Management option	Plugin: Cworkflow

Campaign management

Table 3-31 describes the functionalities that control campaign management.

Table 3-31 Campaign management functionalities

Functionality	Description	Module
Campaign management	Controls settings for all Campaign management functionalities	Plugin: Cworkflow
Change campaign stage	Allows user to change campaign stage	Plugin: Cworkflow
Check if campaign is executable	Checks whether campaign is executable	Plugin: Cworkflow
Delete campaign	Delete campaign	Plugin: Cworkflow
Evaluate campaign	Allows user to evaluate a campaign	Plugin: Cworkflow
Get actions list	Allows user to get an actions list	Plugin: Cworkflow
Get campaign authorizations	Allows user to get campaign authorizations	Plugin: Cworkflow
Get campaign flow information	Allows user to get campaign flow information	Plugin: Cworkflow
Get campaign history	Allows user to get a campaign history	Plugin: Cworkflow
Get campaign lock data	Allows user to get campaign lock data	Plugin: Cworkflow
Get campaigns list	Allows user to get a campaigns list	Plugin: Cworkflow
Get complete campaigns list	Allows user to get a complete campaigns list	Plugin: Cworkflow
Get Media list	Allows user to get a media list	Plugin: Cworkflow

Table 3-31 Campaign management functionalities (continued)

Functionality	Description	Module
Get workflow data	Allows user to get workflow data	Plugin: Cworkflow
Get workflow levels list	Allows user to get a workflow levels list	Plugin: Cworkflow
Load campaign answers	Allows user to load campaign answers	Plugin: Cworkflow
Load campaign data	Allows user to load campaign data	Plugin: Cworkflow
Print campaign evaluation	Allows user to print a campaign evaluation	Plugin: Cworkflow
Protect campaign	Allows user to protect a campaign	Plugin: Cworkflow
Run campaign	Allows user to run a campaign	Plugin: Cworkflow
Save campaign	Allows user to save a campaign	Plugin: Cworkflow
Start campaign	Allows user to start a campaign	Plugin: Cworkflow
Unprotect campaign	Allows user to unprotect a campaign.	Plugin: Cworkflow
Validate the loading of the campaign responses	Allows user to validate a campaign responses load action.	Plugin: Cworkflow
View action	Allows user to view an action.	Plugin: Cworkflow
View medium	Allows user to view a medium.	Plugin: Cworkflow

Campaign planning

Table 3-32 describes the functionalities that control campaign planning management.

Table 3-32 Campaign planning functionalities

Functionality	Description	Module
Campaign planning	Controls settings for all Campaign planning functionalities	Plugin: Cworkflow
Delete strategy	Allows user to delete a strategy	Plugin: Cworkflow
Edit strategy	Allows user to edit a strategy	Plugin: Cworkflow
Get strategies tree	Allows user to access a strategies tree	Plugin: Cworkflow
Load strategy	Allows user to load a strategy	Plugin: Cworkflow
New strategy	Allows user to create a new strategy	Plugin: Cworkflow

Configure CWorkflow

Table 3-33 describes the functionalities that control configure CWorkflow management.

Table 3-33 Configure CWorkflow functionalities

Functionality	Description	Module
Configure CWorkflow	Controls the settings for the following functionalities: <ul style="list-style-type: none"> ■ Levels management ■ Management Actions ■ Media Management ■ Workflow management 	Plugin: Cworkflow
Levels management	Controls the settings for Levels management functionalities	Plugin: Cworkflow
Levels management—Create workflow level	Allows user to create a workflow level	Plugin: Cworkflow
Levels management—Delete workflow level	Allows user to delete a workflow level	Plugin: Cworkflow
Levels management—Edit workflow level	Allows user to edit workflow levels	Plugin: Cworkflow
Management Actions	Controls the settings for Management Actions functionalities	Plugin: Cworkflow
Management Actions—Create new action	Allows user to create a new action	Plugin: Cworkflow
Management Actions—Delete action	Allows user to delete a new action	Plugin: Cworkflow
Management Actions—Edit action	Allows user to edit a new action	Plugin: Cworkflow
<i>(continues)</i>		
Media Management	Controls the settings for Media Management functionalities	Plugin: Cworkflow
Media Management—Create new medium	Allows user to create a new medium	Plugin: Cworkflow
Media Management—Delete medium	Allows user to delete a new medium	Plugin: Cworkflow
Media Management—Edit medium	Allows user to edit a new medium	Plugin: Cworkflow

Table 3-33 Configure CWorkflow functionalities (continued)

Functionality	Description	Module
Workflow management	Controls the settings for Workflow management functionalities	Plugin: Cworkflow
Workflow management—Delete workflow	Allows user to delete a workflow	Plugin: Cworkflow
Workflow management—Edit workflow	Allows user to edit a workflow	Plugin: Cworkflow
Workflow management—Get workflow authorizations list	Allows user to get a workflow authorizations list	Plugin: Cworkflow
Workflow management—Load workflow	Allows user to load a workflow	Plugin: Cworkflow
Workflow management—New workflow	Allows user to create a new workflow	Plugin: Cworkflow
Workflow management—Protect workflow	Allows user to protect a workflow	Plugin: Cworkflow
Workflow management—Unprotect workflow	Allows user to unprotect a workflow	Plugin: Cworkflow
Workflow management—View workflows list	Allows user to view a workflows list	Plugin: Cworkflow
Workflow management—View workflow protection	Allows user to protect a workflow	Plugin: Cworkflow

Events and Alerts

Table 3-34 describes the functionalities that control events and alerts management.

Table 3-34 Events and Alerts functionalities

Functionality	Description	Module
Events and Alerts	Controls settings for all Events and Alerts functionalities	Plugin: Cworkflow/Event Engine
Execute campaign from scheduled task	Allows user to execute a campaign from scheduled task	Plugin: Cworkflow/Event Engine
Export campaign cell	Allows user to exports an action from campaign cell	Plugin: Cworkflow/Event Engine

Table 3-34 Events and Alerts functionalities (continued)

Functionality	Description	Module
Load campaign responses	Allows user to specify loading campaign responses	Plugin: Cworkflow/Event Engine
Notify change of stage	Allows user to specify a stage change notification	Plugin: Cworkflow/Event Engine
Send campaign execution results	Allows user to specify sending campaign execution results	Plugin: Cworkflow/Event Engine

Data Mining

Table 3-35 describes the functionalities that control data mining management.

Table 3-35 Data Mining functionalities

Functionality	Description	Module
Data Mining	Controls settings for all Data Mining functionalities	Plugin: Data Mining
Preprocessing	Controls access to preprocessing capabilities	Plugin: Data Mining
Create dichotomous columns	Controls access to create a boolean column	Frontend: Advanced Analysis Processing

Algorithms

Table 3-36 describes the functionalities that control data mining—algorithms management.

Table 3-36 Algorithms functionalities

Functionality	Description	Module
Algorithms	Controls settings for all Algorithms functionalities	Plugin: Data Mining
Apply C4.5 model	Schedule a C4.5 model application (decision tree or clustering)	Engine and events alerts
Apply KMeans model	Schedule a KMeans model application (decision tree or clustering)	Engine and events alerts
Apply linear regression	Applies a linear regression analysis creating a new column in the database	Frontend Advanced Analysis
Apply logistic regression	Applies a logistic regression analysis creating a new column in the database	Frontend Advanced Analysis
Apply Naive Bayes	Applies a Naive Bayes analysis creating a new column in the database	Frontend Advanced Analysis
		<i>(continues)</i>
Calculate Association Rules	Determine screen visibility for association rules analysis	Plugin: Data Mining
Calculate linear regression	Calculates a linear regression analysis	Frontend: Advanced Analysis
Calculate logistic regression	Calculates a logistic regression analysis	Frontend: Advanced Analysis

Table 3-36 Algorithms functionalities (continued)

Functionality	Description	Module
Calculate time series	Calculate a Holt-Winters analysis	Plugin: Data Mining
Correlation	Calculates a simple correlation analysis between two columns	Frontend: Advanced Analysis
Create Association Rules	Execute association rules analysis	Plugin: Data Mining
Create cluster	Create a model of cluster type	Plugin: Data Mining
Create Naive Bayes	Create a Naive Bayes analysis	Frontend: Advanced Analysis
Create Tree	Create decision tree	Plugin: Data Mining
Execute Time Series Pre-Analysis	Execute a Holt-Winters pre-analysis	Plugin: Data Mining
Export Association Rules	Export association rules analysis	Plugin: Data Mining
Export correlation	Export correlation analysis to CSV file	Frontend: Advanced Analysis
Export linear regression	Export linear regression to CSV file	Frontend: Advanced Analysis
Export logistic regression	Export logistic regression to CSV file	Frontend: Advanced Analysis
Export Time Series	Export Time Series analysis	Plugin: Data Mining
Get Calculated Association Rules	Get association rules analysis	Plugin: Data Mining
Get tree graphical representation	Acquire SVG tree representation	Plugin: Data Mining
Multiple correlation	Calculates a multiple-correlation analysis, (crossed correlation with multiple columns)	Frontend: Advanced Analysis
Test decision tree	Evaluate tree decision	Plugin: Data Mining
Test Naive Bayes	Allows user to test a Naive Bayes analysis	Frontend: Advanced Analysis

Preferences

Table 3-37 describes the functionalities that control preferences management.

Table 3-37 Preferences functionalities

Functionality	Description	Module
Preferences	Controls settings for all Preferences functionalities	Frontend: Start Session

Table 3-37 Preferences functionalities

Functionality	Description	Module
Get password policy	Limits access to the password policy	Admin
Recover security policies	Controls access to the rules required in adding a user password	Frontend: Preferences
View locale	Allows access to the list of available languages	Frontend: Preferences
View topics	Allows access to the topic list	Frontend: Start Session

Statistics

Table 3-38 describes the functionalities that control statistics management.

Table 3-38 Statistics functionalities

Functionality	Description	Module
Statistics	Controls settings for all Statistics functionalities	Frontend: Internal
Analysis statistics	Allows system to maintain statistics of a completed analysis	Frontend: Internal
Get column use information	Obsolete	Frontend: Internal
Get statistics status	Allows administrator to determine if statistics are authorized	Admin